ONLINE RISK ASSESSMENT USING A BANK OF KALMAN FILTERS AND EVENT TREE

by

© Sayyedvahid Bamzad

A Thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Engineering

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

May 2019

St. John's Newfoundland and Labrador

ABSTRACT

Early detection of faults in a process plant is important in order to prevent of happening catastrophic events which might cause deaths, economic, and environmental losses. Recently, on-line calculation of risk and its use for monitoring of process faults were proposed by [Bao et al., 2011]. In this study, a new methodology is proposed which brings more clarity in the calculation of risk from online monitoring of process data. In the proposed methodology, process faults have been classified into two groups: hardware failure and disturbance type faults. First a "Bank of Kalman Filters" is used to detect and diagnose possible failures occurred in the system. Based on the fault category, if it is a disturbance type fault, the estimated states are used directly to calculate the probability of fault. On the other hand, for hardware failure, residuals obtained from Kalman Filter are used to update the probabilities of the affected gates of the "Event Tree", and the probability of occurrence of a catastrophic event is calculated. Next, the risk of operating system under the current condition is calculated using the updated probability and severity. Results show that using the combination of "bank of Kalman Filter" and "Event Tree Analysis" brings more clarity to risk calculation and improves the detection time of the failure. Based on the calculated risk, operators can prioritize the faults and take appropriate action to the most critical one which ensures process safety.

ACKNOWLEDGEMENETS

First of all, I would like to thank my supervisor, Dr. Syed Imtiaz, for the opportunity he gave me to pursue my studies in his research group and for the support and guidance he provided me with during my research. I also gratefully thank my co-supervisors, Prof. Faisal Khan and Dr. Salim Ahmed, for their comments, support and patience.

In the second place, I'm thankful of my parents who have been there for me in my whole life. Without their support, I wouldn't be able to make it through hard times.

Last but not least, I'd like to appreciate my friends support during this study. They've always helped me to keep going and to stay motivated

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

ASCM	Alarm Similarity Color Map
ASM	Abnormal Situation Management
BN	Bayesian Network
CRISE	Centre for Risk, Integrity and Safety Engineering
CSTH	Continuous Stirred Tank Heater
DCS	Distributed Control System
EEMUA	Engineering Equipment and Material Users Association
ETA	Event Tree Analysis
HAZOP	HAZard and OPerability
HDAP	High Density Alarm Plot
ISA	International Society of Automation
KF	Kalman Filter
LOPA	Layer Of Protection Analysis
MPC	Model Predictive Controller
MV	Manipulated Variable
PCA	Principle Component Analysis

PV	Process Variable
SCADA	Supervisory Control and Data Acquisition
SDG	Sign Directed Graph
WSSR	Weighted Sum of Squared Residuals

1 INTRODUCTION

The risk assessment in the process industry is briefly discussed in this chapter. The chapter also states the motivation and objectives of this study.

1.1 Online risk assessment in the process industry

In nowadays process industry, there are thousands of variables in complex plants interacting with each other. Due to the connectivity of these variables, if one variable deviates from its normal operation, the effect can reach the other parts of the plant, and in some cases it can lead to major problems such as explosion, overflow of a tank, etc. So, it's critical to monitor the operation status of the process plant in order to detect any abnormal situation before it leads to a catastrophic event. By technology advancement, the task of monitoring the plant has been automated. However, the task of responding to the abnormal situations in a process plant is still performed by human operator. The task is called Abnormal Event Management (AEM) which involves the early detection of an abnormal event, diagnosing its cause, and take appropriate action to bring the process back to normal condition (Venkatasubramanian et al., 2003a).

To monitor the complex plants with thousands of variables, process control systems such as Supervisory Control and Data Acquisition (SCADA) system and Distributed Control System (DCS) are used in modern process plants. In order to notify the operators about the abnormal situations, warning systems are installed in control rooms to monitor the plant state and detect the deviation of the normal range. Traditional warning systems are

designed to detect the abnormality of single variables. So, for each variable one alarm system is installed. However, in some cases the warning system is unable to detect the deviation of a secondary variable. In such cases, the operator may not be able to detect the possible catastrophic event until the primary variable deviates from its normal range and an alarm being triggered. Early detection of the abnormality, on the other hand, is critical to give the operator enough time to bring the process back to the normal state.

Assigning an alarm for each variable can increase the number of alarms operators receive. Even in the case of minor disturbance, operator gets some secondary alarms due to the noise in the measurement. This can be worse in the case of a major event, when many redundant alarms can be announced before and after the primary alarm. This phenomenon is called “alarm flooding”. Detecting a fault in early stage and reducing the false alarms are main aspects in designing a new warning system. In (Izadi et al. 2009a) a framework is proposed to optimally design the alarm systems. In this framework, three techniques are suggested to reduce the false and nuisance alarm rate: filtering of process data, adding alarm delay and using alarm deadband.

1.2 Motivation and Objectives

Recently, on-line calculation of risk and its use for monitoring of process faults were proposed by Bao et al. (2011). In this study, a new methodology is proposed which brings more clarity in the calculation of risk from online monitoring of process data.

Based on the type of fault occurred in the system, the probability and severity of fault is calculated. Herein, a bank of Kalman filters is used to detect and diagnose different types of faults.

The focus of this thesis is to assess the risk of a faulty system online which is able to annunciate alarms at an early time to give the operator enough time to fix the system. The specific objectives of the thesis are:

- Use a bank of Kalman filters to distinctly detect and diagnose different types of faults occurring in a process system,
- Assess the risk of the process operating under faulty conditions.

In this study, a Bank of Kalman Filters is used to detect and diagnose the faults. Bank of Kalman filter is able to efficiently detect and diagnose the faults occurred in the plant. After that, using Event Tree Analysis (ETA), the probability of occurrence of a catastrophic event is calculated. These probabilities are used to update the risk of operating system under faulty conditions. The whole methodology is briefly discussed in chapter 3.

1.3 Thesis Structure

In the first chapter, the risk assessment was briefly discussed. Chapter 2 reviews the literature comprehensively. Different methods to analyze the risk and methods to detect and diagnose the faults occurred in a system are reviewed in that chapter. Chapter 3 discussed the methodology to assess the risk. Two ``bank of Kalman filters`` are used in order to detect and diagnose sensor and actuator faults. Based on the type of the fault the

risk is calculated using the probabilities and severities of the detected faults. Chapter 4 discusses results for two case studies. A continuous stirred tank heater (CSTH) and the RT 580 fault finding in control systems are used as examples. The concluding remarks and recommendations to improve the work are discussed in chapter 5.

2 LITERATURE REVIEW

In modern manufacturing facilities, there is a large number of variables which interacting with each other under closed-loop control. So, due to complexity and interaction between variables, a failure in one part can propagate to the whole system. Minimizing downtime, increasing the safety of the plant operations, and reducing manufacturing cost can be achieved by early and accurate fault detection and diagnosis. For more heavily instrumented plants, there are more data available for use in detecting and diagnosing faults (Chiang et al., 2001; Bouhoushe et al., 2005; Volosencu 2015).

Producing higher quality products, reducing product rejection rates, and satisfying safety and environmental regulations have been main goals in process and manufacturing industries. Previous process operations are no longer adequate to meet these standards. In order to achieve this goal, in modern industrial processes, variables operate under closed-loop control. The standard process controllers (PID controllers, model predictive controllers (MPC) etc.) compensate the effects of disturbances and changes occurring in the process maintaining the operations in the normal range. On the other hand, there are changes in the process which can't be handled by the controllers. This type of change is called fault. In other words, a fault is an unexpected deviation of any characteristic property or variable from its operating range (Chiang et al., 2001; Volosencu 2015).

Abnormal situations or unexpected process disruptions are the main cause of losses in the process industry. They cost at least $20B in the U.S. industry (Cochran et al., 1996). A range of process disruptions from a minor disturbance to a major process upset are

considered as abnormal situations. These situations require the plant operators to take action as soon as possible to bring the plant back to the normal condition.

There are different types of faults occurring in the system (process parameter changes, disturbance parameter changes, actuator problems, and sensor problems). Heat exchanger fouling, an extreme change in the ambient temperature, a sticking valve, and a sensor biased measurement are examples of process parameter change, disturbance parameter change, actuator problem, and sensor problem, respectively. Detecting, diagnosing and removing the faults are necessary to satisfy the performance specifications, which are associated with process monitoring and Abnormal Situation Management (ASM) (Chiang et al., 2001; Volosencu 2015; Venkatasubramanian et al., 2003a).

Process monitoring includes four procedures: fault detection, fault identification, fault diagnosis, and process recovery. Fault detection is finding if a fault has occurred. Early detection is important to avoid major process problems by giving time to the operator to take appropriate actions. Fault identification is identifying the subsystems and variables most related to the diagnosis of the fault and put plant operator's and engineer's attention on these subsystems and variables. Finding the cause of the unwanted conditions is fault diagnosis which is essential to remove the fault. In process recovery procedure, the effects of the faults are removed (Chiang et al., 2001; Volosencu 2015).

Advanced sensor development and control technology has improved the efficiency and productivity in the process industries (Tao et al., 2017). However, these technologies are not able to eliminate the abnormal situations. So, the operators have to continuously intervene to correct the abnormal situations (Cochran et al., 1996).

In order to early detection of an abnormal situation, warning systems have widely been used in process industries (Lu et al., 2018, Jain et al., 2018). These systems are able to detect a deviation from normal operating conditions and notify the operator to take proper action in order to bring the system back to the normal conditions. The warning system is considered as the 3rd layer in the layer of protection analysis (LOPA) (Crowl & Louvar, 2001). These systems have an important role in the plant safety by informing the operators. They can be defined as the mechanisms run in a plant to inform the personnel about the risk of a possible danger before it happens. In other words, the warning system gives the operator enough time to be prepared for a danger or make a decision to reduce the effects of the events or even prevent them (Hotz et al., 2006).

There have been many types of these systems used in the process industry. The warning systems trigger an alarm in the case of an abnormal situation. In some processes, there are many alarms triggered at the same time due to safety consideration. The number of alarms increases in some cases which are more than what even an experienced operator can handle (Yang et al., 2012). So, "alarm rationalization" has been the main focus of recent projects in industry, which is detecting the abnormal situations while trying to reduce the number of false alarms at the same time. In this process, the design requirements of alarms are considered based on plant alarm philosophy; that means the alarm setting, consequences of deviation, and the corrective action the operators have to take are taken into account (Izadi et al., 2009a; Hollender & Beuthel, 2007). Izadi et al. (2009a) proposed a framework to optimally design the alarm system. Filtering of process

data, adding alarm delay and using alarm deadband are considered as useful techniques to reduce the false alarms.

Alarm management has been considered as one of the main tasks in all industries. The Engineering Equipment and Materials Users Association (EEMUA) has published a guideline to properly design, manage and procure of alarm systems known as EEMUA 191 (EEMUA, 2007). Based on this guideline, a warning system should be: unique, relevant, timely, understandable, prioritized, focusing, and diagnostic. A similar milestone was published by International Society of Automation (ISA) which is known as ISA 18.2 Standards (ISA, 2009). Some standards for alarm systems are provided in ISA 18.2 such as: definition, design, management, and installation. Both EEMUA 191 and ISA 18.2 show the proper efforts and tasks required to effectively design an alarm system.

There are different types of alarms defined based on necessity (ISA, 2009):

- Absolute alarms,
- Deviation alarms,
- Rate of change alarms,
- Statistical alarms,
- Discrepancy alarms,
- Controller output alarms,
- Instrument diagnostic alarms, and
- Bad measurement alarms.

These types of alarms can be classified as: continuous alarms and digital alarms. The former one is associated with continuously measurable variables such as: pressure, flowrate, and temperature; the digital alarms are associated with logical decisions such as: instrument failure, valve malfunction, and measurement failure. In continuous alarms, a limit is designed based on: distribution of process variable, maximum rate of change, average response time, the amount of risk involved, and process condition model (EEMUA, 2007). When a variable deviates from each assigned limit, an alarm is triggered having an identifier. The most common identifiers used with continuous alarms are: high (identified as PVHI), low (identified as PVLO), high-high (identified as (PVHH) and low-low (identified as PVLL).

Common warning systems which are used mostly in the industry are variable based systems. In this type of systems, if it is possible, an alarm is assigned for each variable. So, an alarm is triggered when the value of a single variable deviates from its normal range. Due to connectivity of variables in a plant, any change in one variable can make changes in other variables as well. Consequently, when one variable crosses its threshold limit, there could be many other variables go beyond their normal range and make many alarms to be triggered which some of these alarms are false or nuisance alarms (Izadi et al., 2009a; Izadi et al., 2009b). This occurrence is known as alarm flooding (Yang et al., 2012; ISA, 2009). In the ISA 18.2 alarm flooding is defined as (ISA, 2009):

"A condition during which the alarm rate is greater than the operator can effectively manage (e.g. more than 10 alarms per 10 minutes)."

Based on EEMUA 191, the approximate time an operator needs to effectively manage an alarm is 10 minutes and the rate of alarms shouldn't be more than 60 alarms per hour (EEMUA, 2007). But, in reality, the alarm rate exceeds this standard value. Table 2-1 shows a comparison between EEMUA standards and what happens in some industries (Izadi et al., 2009b)

Table 2-1: EEMUA standards and average values happen in industry (Izadi et al., 2009b)

	EEMUA	Oil and Gas	Petrochemical	Power
Average alarms/hr	≤6	36	54	48
Average standing alarms	9	50	100	65
Peak alarms/hr	60	1320	1080	2100
Distribution % (low/med/high)	80/15/5	25/40/35	25/40/35	25/40/35

ISA 18.2 recommends some similar standards for the maximum time an alarm system can be in flood. It recommends that an alarm system shouldn't be in flood more than one percent of reporting time which is far away from what happens in reality. Advanced alarming techniques can be considered to study and analyze alarm floods. ISA 18.2 classified these techniques into 4 different categories:

- Information based alarming
- Logic based alarming
- Model based alarming, and
- Additional alarming consideration

Alarm management is a relatively new area in process control. In early stage of designing a new plant, one crucial step is finding the necessary points for which an alarm is required (Yan et al., 2007a). The studies on alarm management and design in process industry can be classified as two categories: single variable alarm design and multivariate alarm analysis. The former one is an essential step to effective alarm design. The alarms are set on either process variables (PVs) or manipulated variables (MVs) (Yan et al., 2007b). Due to presence of noise, different operating conditions, and instrumentation limitation, these variables have dispersions in their statistical distributions which can cause high false or missed alarm rates (Izadi et al., 2009a; Izadi et al., 2009b; Kang & Seong, 1999). Data filtering, adding alarm delay, using deadband and alarm window design are some techniques to overcome this issue (Izadi et al., 2009a).

There are numerous variables in an industrial plant which makes it difficult to analyze and design an alarm for each single variable. So, it is more effective to use multivariate alarm systems.

There are many multivariate fault detection methods proposed to early fault detection and diagnosis. These methods can be classified as: quantitative model based methods, qualitative model based methods and historical data based methods (Venkatasubramanian et al., 2003a, 2003b, and 2003c). In the quantitative model based approaches, a first principle model is required to estimate the state of the process variables. Kalman Filter is a powerful tool frequently used in this approach. Zadakbar et al. (2013) used the residuals generated from Kalman Filter to detect the faulty conditions in a process plant. On the other hand, due to the complexity of a real plant, developing a first principle model is

difficult. In qualitative mode based approach, a causal model such as fault tree is used to detect the faults. In these techniques, alarms and variables in a process are grouped based on their interrelations (Yang et al., 2012; Kondaveeti et al., 2010). Root cause determination is achieved using causality analysis of interrelated variables. In a causality analysis, information theoretic approaches are used in order to determine a cause and its effects from a time series data (Hlavackova et al., 2007; Barnett et al., 2009). Different approaches have been used for root cause analysis in process industry using transfer entropy (Bauer et al., 2007), reachability (Yang et al., 2009), and sign directed graph (SDG) (Yang et al., 2010). However, the capability of these qualitative approaches to detect the fault in real time is limited. As an alternative to the fist principle approach, the historical data based methods have been proposed in literature. There are some relationships between different variables in a system. Using multivariate analysis, some information can be extracted from a large number of variables and be expressed by a smaller number of latent variables (Izadi et al., 2009b). These virtual variables are calculated by combining other variables. Principle Component Analysis (PCA) is a multivariate technique which reduces the number of false and missed alarms by assigning alarms on fewer variables based on Q and T^2 statistics of many other variables (Kondaveeti et al., 2009; Zadakbar et al., 2012). One difficulty arises using these methods is that developing a statistical model needs a large set of historical data.

Some visualization tools using the High Density Alarm Plot (HDAP) and the Alarm Similarity Color Map (ASCM) have been used to identify the nuisance alarms (Kondaveeti et al., 2010). Event correlation analysis (Noda et al., 2011) and fuzzy

clustering methodology (Zhu & Geng, 2005) have been studied in order to identify the similarity among alarms to reduce the nuisance alarms.

As a probabilistic graphical method, Bayesian Network (BN) has been used in some studies (Argiolas et al., 2012; Hossain & Muromachi, 2012). BN is a powerful tool which is capable of doing fault diagnosis under uncertainty. BN was used in safety analysis method proposed by Khakzad et al. (2011)

Recently, as an alternative to variables based alarm system, risk-based alarm methodology has been studied (Bao et al., 2011). In this approach, an alarm is assigned to be triggered when the risk of associated event exceeds a predefined threshold. Risk is defined as a function of the probability of occurrence of an event and its consequences. In the proposed methodology, authors used a univariate approach which has limited capability to reduce the false alarms. Ahmed et al. [2011] extended the methodology by proposing an event-based alarm system. They proposed instead of defining the risk for each variable, an alarm is triggered when the risk of an event goes beyond the threshold. In the mentioned studies on risk-based alarm systems, it's not said how to calculate the probabilities and the severities of an event. In current study, event tree analysis is used to calculate these parameters.

3 METHODOLOGY

In the current study, a new methodology is proposed to assess the risk of system operating under faulty conditions. The proposed methodology is consisted of two sections: a) fault detection and diagnosis, and b) risk assessment. Figure 3-1 shows the flowchart of the proposed methodology.

The first step in the methodology is finding a model describing the system. To find such a model, the previous operating data are used. The more the available data are, the better the model is. This model can be updated as some new data are gathered. The State Space (SS) model of the system can be found using System Identification Toolbox of MATLAB.

Having this model, new data, obtained from different sensors assigned on different variables, are applied to find if the system is working under normal condition or a fault has occurred in the system.

Fault detection and diagnosis is an important step regarding the safety improvement in a complex industrial process. The three essential tasks involved in the fault diagnosis are: fault detection, fault isolation and fault identification. The first task detects the occurrence of a fault in the process; fault isolation classifies the different faults and fault analysis determines the type, magnitude and the cause of the fault (Ding, 2008).

There are many different approaches regarding fault detection techniques. These methods can be classified in three categories: quantitative model based approach, qualitative model

based approach and historical data based approach (Venkatasubramanian et al., 2003a, 2003b, and 2003c).

A common part in all developed model based techniques is using a process model. Using the processing data, which are collected online during the plant operation, the fault detection and diagnosis algorithms are implemented based on this model (Ding, 2008).

Advanced computer technology and the control techniques along with technological and economic demands have made the model based fault diagnosis approach as a powerful tool to solve fault diagnosis problems. The schematic description of the model based fault diagnosis approach is shown in Figure 3-2 (Ding, 2008). As seen in this figure, an important part of this approach is residual generation. One popular method to generate residuals, which has been used in the current study, is the Kalman filter which is briefly discussed in the next section.

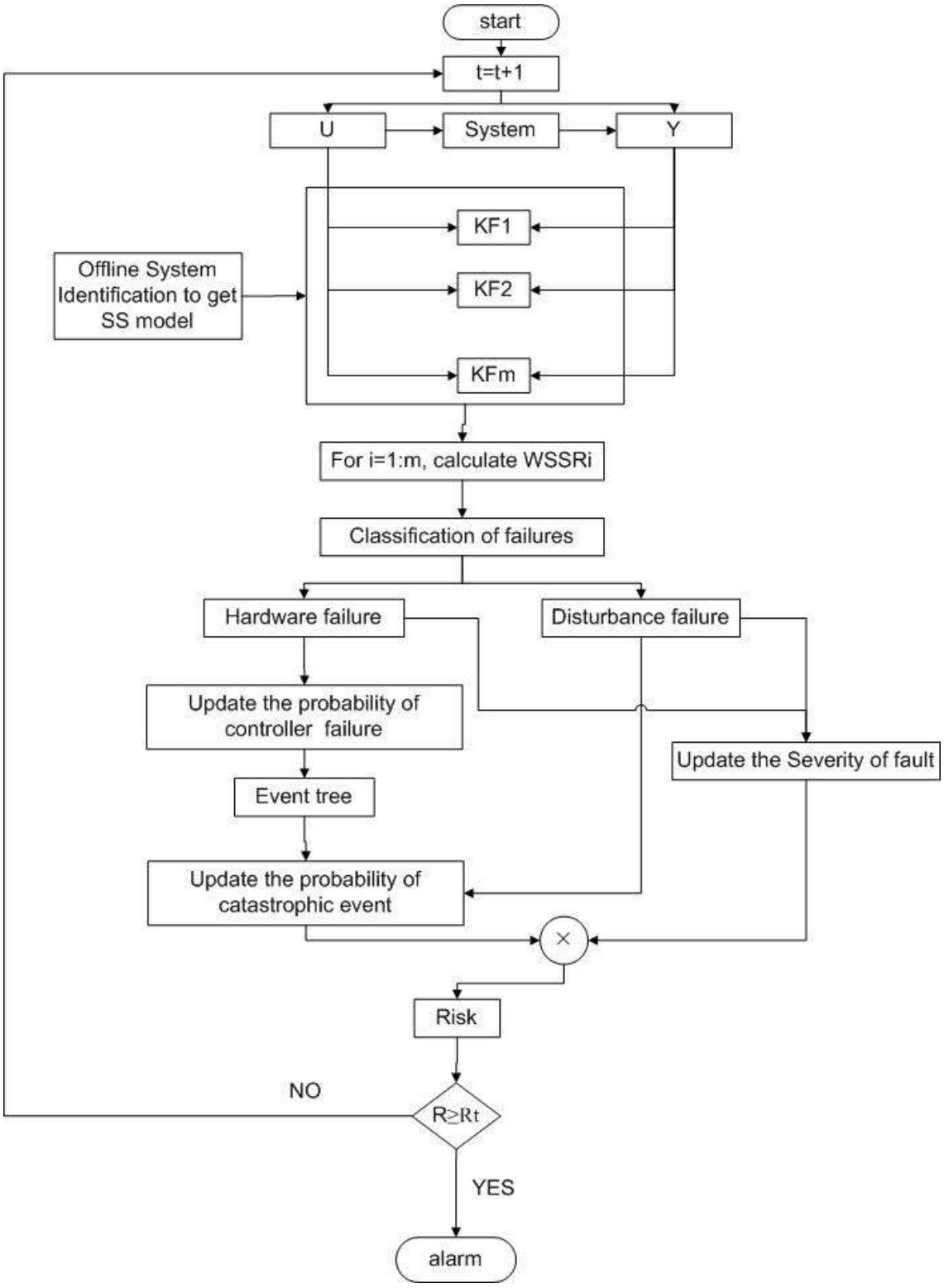

Figure 3-1: Implementation steps of the proposed methodology

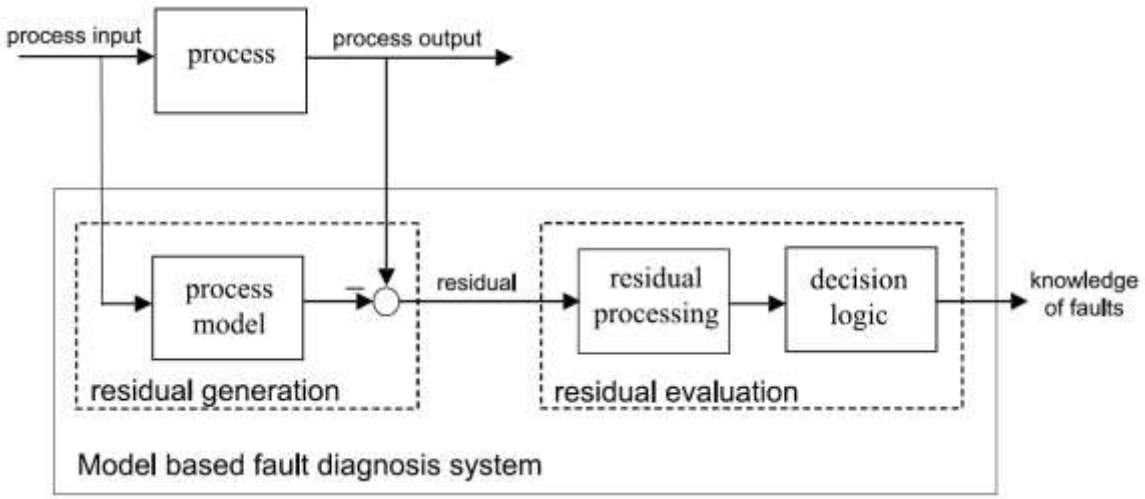

Figure 3-2: the schematic description of the model based fault diagnosis technique (Ding, 2008)

Here, a bank of Kalman filters are used to distinguish between different sensors or actuators faults. The number of Kalman filters is the summation of sensors and actuators in the system. There is also another Kalman filter which assumes that the system is under normal conditions at all the time. The main model is modified for sensor/actuator which is discussed later on this chapter. These filters are used to predict the states of the model at each time which are used to calculate the probability of failure.

Each Kalman filter defines a hypothesis that assumes the associated sensor/actuator is faulty. To find if the hypothesis is right or not, for each Kalman filter, a fault indicator is defined as the Weighted Sum of Squared Residuals (WSSR). Once these indicators are calculated, the accuracy of hypotheses is validated and the occurrence of a fault is detected.

Next step in the methodology is to classify the type of faults. Here, two types of failure are defined: hardware failure and disturbance failure. Sensor failure and actuator failure

are categorized as hardware failure. The reason to distinguish between different types of failure is that to find the probability of failure different methods are used for hardware and disturbance failures. For hardware failure, the fault indicators are used to update the probability of failure at each time, and state predictions are applied in the case of a disturbance failure.

These updated probabilities are applied to an Event Tree (ET) to calculate the probability of occurrence of a major event. An Event Tree is a graphical representation of different scenarios knowing that an initiating event has already happened in the system. The Event Tree Analysis (ETA) will be briefly discussed in the next sections.

The consequence (severity) of each fault is calculated simultaneously. Usually the severity of a fault is a function of different parameters (e.g. the severity of an explosion is higher when more people are working on a plant rather than when no one is at the location of the explosion). Herein, the only factor considered in calculating the severity of a fault is residuals obtained from associated Kalman filter.

Having the probability of a major event and the severity of the fault, the risk of system operating under current conditions is updated at each time. If the calculated risk exceeds a predefined threshold, an alarm will be triggered to bring operator's attention to the faulty location. On the other hand, if the risk remains below the critical point, no alarm will be announced. In that case, the number of false alarms is reduced.

Different steps of the methodology are briefly discussed in the following sections.

3.1 Kalman Filter

The Kalman filter is an efficient method to generate residuals in which the linear model of a plant is used. Considering the following discretized linear time invariant model:

$$\begin{cases} X_k = A_k X_{k-1} + B_k U_{k-1} + W_k w_k \\ Y_k = C_k X_k + V_k v_k \end{cases} \quad (3\text{–}1)$$

in which, $k \in \mathbb{N}$ shows the time index and $x_k \in \mathbb{R}^n$ is the state; $U_k \in \mathbb{R}^l$ and $Y_k \in \mathbb{R}^m$ are noise-free input and noisy output; $w_k \in \mathbb{R}^n$ and $v_k \in \mathbb{R}^m$ are stationary Gaussian white noise vectors with covariance $Q \in \mathbb{R}^{n\times n}$ and $R \in \mathbb{R}^{m\times m}$, for example $w_k \sim \mathcal{N}(0, Q)$ and $v_k \sim \mathcal{N}(0, R)$, to represent process disturbances and measurement noise, respectively; system matrixes A_k, B_k, C_k, W_k, and V_k have proper dimensions. Taking into account the possible faults occurring in different parts of the system, Eq. (3-1) needs to be modified. Considering the process fault, new equations can be as:

$$\begin{cases} X_k = A_k X_{k-1} + B_k U_{k-1} + F_k f_{pk} + W_k w_k \\ Y_k = C_k X_k + V_k v_k \end{cases} \quad (3\text{–}2)$$

In which, the new term, $F_k f_{pk}$, shows the process fault.

In Kalman filter approach, the residuals are used for fault detection and diagnosis. At any time, the residuals are calculated as the following equation:

$$r_k = y_k - \hat{y}_{k|k-1} \quad (3\text{–}3)$$

In Eq. (3-3), k is the time instant, y_k and $\hat{y}_K$ are the measurement and corresponding predicted values at time instant k. In many studies, the Kalman filter based residual generation method has been used to get the residuals (Zadakbar et al., 2013; Hsoumi et al., 2009). In the case of a linear system with Gaussian noise, the Kalman filter gives the

optimal state estimation. It is also robust considering disturbance and uncertainty in the process.

For a linear system with known matrixes and Gaussian process and measurement noise, least square estimate of x_k is obtained using the Kalman filter; Kalman filter gives minimum variance for $x_k - \hat{x}_{k|j}$ in which $\hat{x}_{k|j}$ is the estimation of x_k using previous inputs and outputs, $\{u(1), y(1), \dots u(j), y(j)\}$, where $j = k - 1$, for predicting one step ahead, or $j = k$ for filtering (Li et al., 2008). The predictor algorithm of Kalman filter is:

$$\begin{cases} \hat{X}_{k+1|k} = A\hat{X}_{k|k-1} + BU_k + K_k\tilde{Y}_k \\ \hat{Y}_k = C\hat{X}_{k|k-1} \end{cases} \quad (3-4)$$

Where, the Kalman gain, K_k, is given as:

$$\begin{cases} K_k = P_k^- C^T (CP_k^- C^T + R)^{-1} \\ P_k^- = E\left[e_k^- e_k^{-T}\right] \\ e_k^- = x_k - \hat{x}_k \end{cases} \quad (3-5)$$

In the case of process fault, the residuals are calculated using the following equation:

$$r_k = \left[\left(C_k F_k f_{pk} + C_k W_k w_k + C_k V_k v_k\right) - C_k K_k \tilde{Y}_k\right] \quad (3-6)$$

In order to remove noise, the residuals calculated from Eq. (3-6) are filtered using exponential filtering method, as the following equation:

$$r_k = \alpha r_k + (1 - \alpha) r_{k-1} \quad (3-7)$$

In this equation, α is the filter coefficient which can be tuned to minimize false alarms.

The concept of getting residuals using Kalman Filter is shown in Figure 3-3.

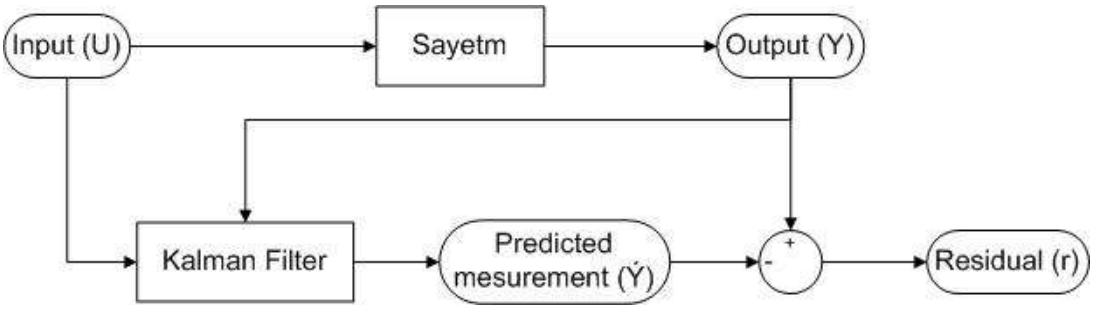

Figure 3-3: Residual Generation using Kalman Filter

The Kalman filter has been used to detect and diagnose faults. There are different types of faults occur in a system which can be classified as: hardware failure (e.g. sensor failure and actuator failure) and disturbance failure. To distinguish between different failures the concept of "bank of Kalman filters" has been applied.

3.2 Sensor Fault Detection

In order to detect and diagnose a sensor fault using a "Bank of Kalman Filters", m Kalman filters are designed where m represents the number of monitored sensors. Each Kalman filter uses all sensor measurements except one (m-1 sensor measurements) which is assumed to be the faulty sensor. In other words, each Kalman filter is designed with the hypothesis that detects the faulty sensor. For example, the i^{th} Kalman filter uses the set of sensor measurements y^i in which the i^{th} sensor measurement is excluded. In the case of i^{th} sensor fault, all Kalman filters use faulty measurements except the i^{th} filter (Kobayashi & Simon, 2004).

On the other hand, while there is no faulty data in i^{th} filter, it accurately estimates the states. The states and predicted outputs for i^{th} Kalman filter are calculated using the following equation:

$$\begin{cases} X_k = A_k X_{k-1} + B_k U_{k-1} \\ \widehat{Y}_k^i = C_k^i X_k \end{cases} \quad (3-8)$$

In which, the matrix C_k^i is obtained by removing the i^{th} row of matrix C_k.

A weighted sum of squared residuals (WSSR) is used to detect and diagnose a sensor failure, which is calculated as:

$$WSSR_s^i = \left(Y^i - \widehat{Y}^i\right)^T \left(\Sigma^i\right)^{-1} \left(Y^i - \widehat{Y}^i\right) \quad (3-9)$$

Where, Σ^i is a square matrix to normalize the residual vector$\left(Y^i - \widehat{Y}^i\right)$, and it is computed as:

$$\Sigma^i = \text{diag}\left[\sigma^i\right]^2 \quad (3-10)$$

In this equation, σ^i is the standard deviation vector of the i^{th} sensor-subset. The i^{th} sensor fault indicator signal, $WSSR_s^i$, uses all sensor measurements except the i^{th} sensor value. If the sensor subset used by i^{th} Kalman filter contains a faulty value, the associate fault indicator signal increases. In other words, in the case of i^{th} sensor fault, the value of the fault indicator signal exceeds a predefined threshold for all Kalman filters except for the $WSSR_s^i$. In this case, the sensor fault is detected and identified (Kobayashi & Simon, 2004).

One important assumption is that, at any time, only one sensor failure occurs. Figure 3-4 shows the structure of the sensor FDI system. In this structure, m indicates the number of monitored sensors.

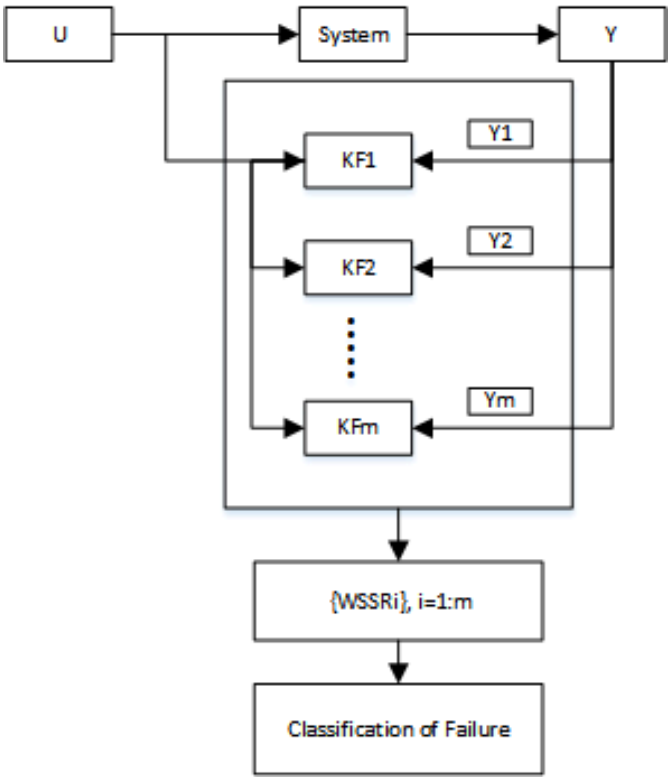

Figure 3-4: Sensor Fault Detection and Diagnosis procedure using Bank of Kalman Filter

Different types of sensor failure have been considered in this study as:

- Total failure (sensor stops working and gives zero output),
- Stuck Failure (sensor outputs remains constant),
- Bias Failure (a constant value is added to sensor output), and
- Noisy failure (sensor output gets additional noise)

3.3 Actuator Fault Detection

While Eq. (3-8) doesn't account the actuator bias or component parameters, any change in these parameters can influence the fault indicator signals. So, there is a need to find another filter to detect this kind of fault and distinguish it with sensor faults.

In order to detect and diagnose the actuator failures, n Kalman Filters are designed, where n is the number of actuators in the system. For each filter, the states and predicted output are calculated using the following equations (Rago et al., 1998):

$$\begin{cases} X_k = A_k X_{k-1} + B_k^i U_{k-1} \\ Y_k = C_k X_k \end{cases} \quad (3-11)$$

Here, matrix B_k^i is obtained by zeroing the i^{th} column of matrix B. In other words, in the set of Kalman filters designed for detecting actuator failure, the i^{th} filter doesn't take into account the input to the i^{th} actuator. So, in case of i^{th} actuator failure, all Kalman Filters use faulty inputs except the i^{th} one which is designed to detect and diagnose the i^{th} actuator fault. The actuator fault indicator, $WSSR_a^i$, is defined as:

$$WSSR_a^i = \left(Y^i - \hat{Y}^i\right)^T \left(\Sigma^i\right)^{-1} \left(Y^i - \hat{Y}^i\right) \quad (3-12)$$

in which, the normalizing matrix, Σ^i, is calculated using Eq. (3-10). Here, all sensor measurements are used. If i^{th} actuator fails, all actuator fault indicator increase except i^{th} one.

The methodology proposed here is able to detect the disturbance failure. While m+n Kalman Filters are designed to detect and diagnose the sensor/actuator failure, if a disturbance failure occurs, all fault indicators increase. Table 3-1 represents different scenarios based on fault indicators.

Table 3-1: the summary of fault detection and diagnosis approach based on fault indicators

	All $WSSR_a$ remain below the predefined threshold	All $WSSR_a$ but the j^{th} exceed the predefined threshold	All $WSSR_a$ exceed the predefined threshold
All $WSSR_s$ remain below the predefined threshold	No fault	NA	NA
All $WSSR_s$ but the i^{th} exceed the predefined threshold	NA	NA	The i^{th} sensor failure is detected and diagnosed
All $WSSR_s$ exceed the predefined threshold	NA	The j^{th} actuator failure is detected and diagnosed	Disturbance failure

3.4 Risk Quantification

Risk is defined in Oxford Dictionary as "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstances; a chance or situation involving such a possibility" (OED Online, 2016). It can be defined as the likelihood of occurrence a hazardous event. Quantifying the risk consists of two factors: the probability of happening an unwelcome event, and the severity or consequences caused by that event (Zadakbar et al., 2013). Eq. (3-13) is proposed to calculate the risk for a univariate deterministic system (Bao et al., 2013):

$$Risk = P \times S \qquad (3-13)$$

In this formula, P stands for the probability of hazardous event to happen, and S represents the severity. When the process deviates from normal operation, the probability of occurrence an unwanted event increases. Using residuals obtained from Eq. (3-3), the probability and severity are calculated by Eq. (3-14) and Eq. (3-15), respectively. In these equations, the upper and the lower bounds for normal operating range are chosen as

$\mu + 3\sigma$ and $\mu - 3\sigma$. If the generated residuals deviate from this normal range, a hazardous event is likely to happen. For residuals at threshold points, $\mu \pm 3\sigma$, the probability of happening a fault is 0.5, which means the process can go to faulty condition or come back to normal operation. As shown in Eq. (3-14), for positive or negative fault signals, the probability of fault is calculated by $\varphi\left(\frac{r-(\mu+3\sigma)}{\sigma}\right)$ and $1-\varphi\left(\frac{r-(\mu-3\sigma)}{\sigma}\right)$, respectively.

$$\begin{cases} r_k > \mu \rightarrow P = \varphi\left(\dfrac{r_k-(\mu+3\sigma)}{\sigma}\right) = \displaystyle\int_{-\infty}^{r_k} \frac{1}{\sqrt{2\pi}\sigma} e^{-\left(\frac{\left(r-(\mu+3\sigma)\right)^2}{2\sigma^2}\right)} dr \\ r_k < \mu \rightarrow P = 1-\varphi\left(\dfrac{r_k-(\mu-3\sigma)}{\sigma}\right) = 1-\displaystyle\int_{-\infty}^{r_k} \frac{1}{\sqrt{2\pi}\sigma} e^{-\left(\frac{\left(r-(\mu-3\sigma)\right)^2}{2\sigma^2}\right)} dr \end{cases} \quad (3-14)$$

The residuals are also used to calculate the severity of fault as:

$$\begin{cases} r > \mu \rightarrow S = 100^{\frac{r-(\mu+3\sigma)}{r-\mu}} \\ r < \mu \rightarrow S = 100^{\frac{r-(\mu-3\sigma)}{r-\mu}} \end{cases} \quad (3-15)$$

At each time instant, having the probability and severity of the fault, the risk is calculated using Eq. (3-13). When the risk exceeds a predefined threshold, a fault is detected and proper decisions are taken to take the system to a safe condition.

3.5 Event Tree

Event Tree is an analysis technique to analyze the outcomes of failing or functioning of different parts of the system given that an event has already occurred (Wang & Roush, 2000). This technique consists of the following steps (Crowl & Louvar, 2001; Ferdous, 2011):

A. Identification of Initiating Event: The first step in Event Tree analysis is to identify the initiating event which is an event that starts the path to a catastrophic event (e.g. spark, lightning, gas release, a change in flow-rate etc.),

B. Identification of Safety Barriers: The safety barriers are designed to prevent of occurrence a catastrophic event or to mitigate the effects of failure. They are functioning according to the order they are needed to prevent or mitigate. The barriers which are referred to as the prevention layers are designed to reduce the probability of occurrence a hazardous event. Some safety barriers are listed as follow:

- Process Plant Design

The design stage of a plant can be considered as a safety barrier. There are a lot of HAZOP studies (HAZard and Operability studies) implemented during designing time of a plant to design it as safe as possible (Ishtiaque et al., 2017; Ora et al., 2017), .

- Process Control System

When a plant is operating, the process control system is the first safety barrier. It can bring the variables (e.g., level, temperature, pressure, etc.) back to the normal operating range if they deviate. In some cases, the deviation is so big that the control system is unable to keep the variables in normal range. In these cases, the control system failure is considered as an initiating event.

- Alarm System

As mentioned before, the process control system may fail to function. In such a case, alarms could be announced to inform the operators that a problem has happened in the system. Alarms could be designed based on different approach (e.g., variable based design, event based design, etc.) (Dalaptadu, 2014). Any alarm system should have some properties:

- It should detect problems as early as possible, giving plant's operators and personnel enough time to take appropriate action to bring the plant back to safe condition.
- It should be independent of the system for which the alarm system is designed (i.e., system failure should not affect the alarm system).
- It should be simple to implement.
- Its maintenance should be easy.

➢ Plant's Operators and Personnel

While the plant is complex and large scale, there are some unexpected conditions occurring in the plant. On the other hand, there are some tasks which are impossible to be automated. In certain situations, human operators are needed in place for their flexibility to fix some problems happening in the system. In such cases, operators can be considered as a protective layer.

➢ Shutdown System /Safety Instrumented System (SIS)

In some cases, none of mentioned barriers works their functions. In such cases, to prevent a hazardous event, the system needs to be shut down. If operator fails to shut down the

system manually, it should be designed to happen automatically. Usually, automatic shutdown systems are separated from other parts of the system. They use different sensors and logic systems. Automatic shutdown system should perform the following functions:

- They don't work when system variables are in normal and safe range,
- When normal conditions are violated, this system should automatically become active to take the process to a safe condition, or mitigate the consequences

C. Event Tree Construction:

When the initiating event and safety barriers are identified, event tree is constructed as:

- ✓ Input The Initiating Event: Event Tree starts with a horizontal arrow to represent the initiating event,
- ✓ Place the Safety Barriers: Starting from the initiating event, event tree can go to two ways which mean the failure or success of the first barrier (e.g., usually the top way stands for the success and the bottom one represents the failure),
- ✓ For each way, next step should be decided based on HAZOP study
- ✓ For each path, the safety barriers are evaluated qualitatively to find the consequences of different conditions (e.g., what happen if specific barriers fail or succeed to perform their function).

D. Classify Accident Outcomes: When the consequences of different branches in the event tree are found, they are classified to show the possible outcomes

E. Estimate and rank outcomes probability: Having the initiating event frequency and the probability of failure of the barriers the frequency of all outcomes are estimated.

An example of an Event Tree is shown in Figure 3-5. In this figure, S means that the safety barrier functions properly and when it fails to function, the branch is shown by F. Some outcomes could be the same in the event tree. In this research the failure of first barrier which is controller failure has been studied. Based on controller failure the failures are classified.

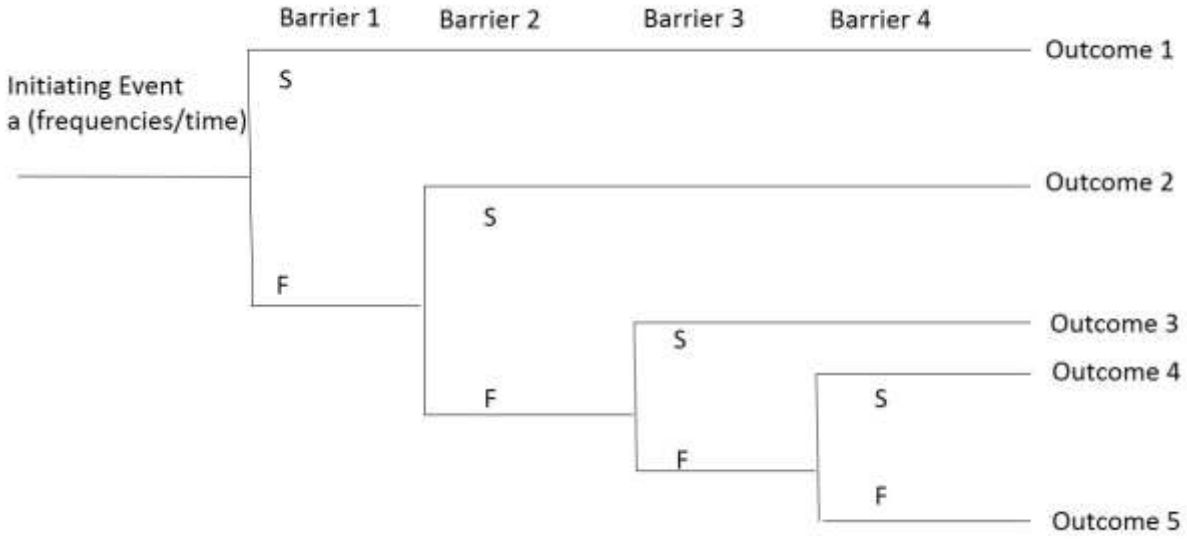

Figure 3-5: Schematic of an Event Tree

4 RESULTS AND DISCUSSION

The proposed methodology has been applied to two case studies: a Continuous Stirred Tank Heater (CSTH) and the RT 580 fault finding in control systems.

4.1 Continuous Stirred Tank Heater (CSTH)

The proposed methodology is applied to a continuous stirred tank heater (CSTH) (Thornhill et al., 2008). In this example, system modeling uses experimental data making the model more realistic. In order to apply the methodology, the Simulink model of the plant is used (Thornhill et al., 2007).

The schematic diagram of the plant is shown in Figure 4-1. The cold water stream is heated by steam and hot water streams. The level of the water in the tank is controlled by manipulating the cold water flow. Level controller is cascaded with flow controller to control the cold water flow. The temperature of the tank, assumed to be the same as the temperature of the outflow stream, is controlled by manipulating the steam valve. The process dynamics are discussed in detail in (Thornhill et al., 2008). The volume of the tank is 8 l with circular cross section and the height of 50 cm.

The continuous state space model of the plant is represented as:

$$\begin{cases} X' = AX + BU \\ Y = CX \end{cases} \qquad (4-1)$$

In which,

$$\begin{cases} U = \begin{bmatrix} u1 \\ u2 \\ u3 \end{bmatrix} = \begin{bmatrix} \text{Cold Water Valve Position} \\ \text{Steam Valve Position} \\ \text{Hot Water Valve Position} \end{bmatrix} \\ Y = \begin{bmatrix} y1 \\ y2 \\ y3 \end{bmatrix} = \begin{bmatrix} \text{Level} \\ \text{Cold Water Flow} \\ \text{Temperature} \end{bmatrix} \end{cases}$$

In the above equations, matrices A, B, and C are (Thornhill et al., 2008):

$$A = \begin{bmatrix} -3.7313 \times 10^{-3} & 1.5789 \times 10^{-6} & 0 \\ 0 & -2.6316 \times 10^{-1} & 0 \\ 4.1580 \times 10^{3} & 1.5842 \times 10^{-1} & -2.7316 \times 10^{-2} \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 4.29 \times 10^{-5} \\ 1 & 0 & 0 \\ 0 & 6.4 \times 10^{-1} & 8.8712 \end{bmatrix}$$

$$C = \begin{bmatrix} 2690 & 0 & 0 \\ 0 & 1.5132 \times 10^{-1} & 0 \\ -1979.2 & 0 & 1.1226 \times 10^{-2} \end{bmatrix}$$

Table 4-1 shows the steady state values and conditions for the operating point. Here, cold water valve and temperature measurements have time delay of 1s and 8s, respectively. In this table, the units in mA and metrics are presented. The values in mA range from 4 to 20. For example, if the value of a variable is 4 mA, its metrics value is 0.

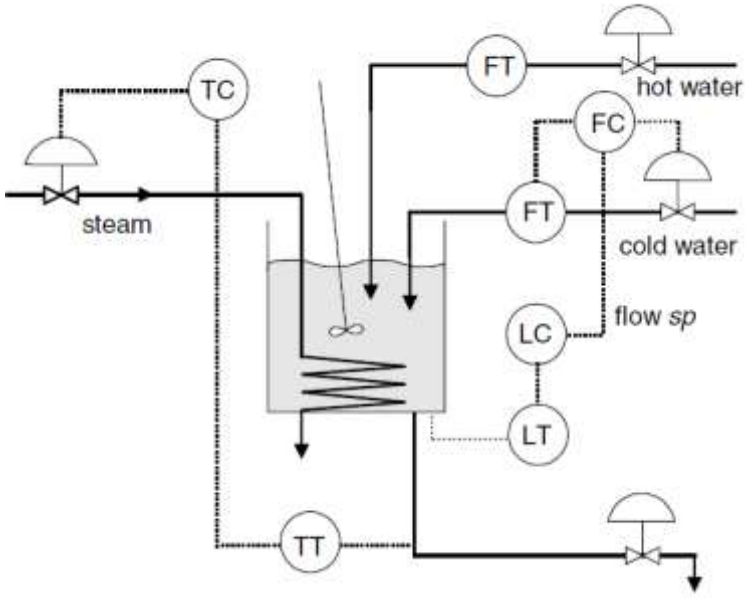

Figure 4-1: schematic diagram of the CSTH plant (Thornhill et al., 2008)

Table 4-1: Operating point for CSTH (Thornhill et al., 2008)

Variable	Operating Point
Level/mA	12.00
Level/cm	20.48
CW flow/mA	7.330
CW flow/m^3s^{-1}	3.823×10^{-5}
CW valve/mA	7.704
Temperature/mA	10.50
Temperature/˚C	42.52
Steam valve/mA	6.053
HW valve/mA	5.500
HW flow/m^3s^{-1}	5.215×10^{-5}

4.1.1 Fault Detection and Diagnosis for CSTH

The CSTH has 3 sensors for level, cold water flow and temperature, so 3 Kalman filters were designed to detect and diagnose failure in each sensor. There also are two actuators in the system: CW valve, which is manipulated to control the level of the system, and steam valve, which is manipulated to control the temperature of the tank. To distinguish between sensor and actuator failure, two additional Kalman filters were designed. An additional Kalman filter, KF0, with the hypothesis that the system is under normal conditions is designed. Table 4-2 shows the designed Kalman filters and hypotheses associated with them. MATLAB software is used to implement the programming.

Table 4-2: Designed Kalman filters for CSTH

Kalman Filter	Hypothesis
KF1	Level sensor is faulty
KF2	CWF sensor is faulty
KF3	Temperature sensor is faulty
KF4	CW actuator is faulty
KF5	Steam actuator is faulty
KF0	The system is not faulty

There are 12 possible sensor failure scenarios (total failure, stuck failure, noisy failure and bias failure for each sensor) and two actuator failure scenarios, by the assumption that at each time only one failure occurs. All failure scenarios are summarized in Table 4-3.

Table 4-3: Possible failure scenarios for CSTH

Failure number	Failure scenario	Description
F1	Partial failure of level sensor	Level sensor gets stuck at the value of 11.99 mA
F2	Total failure of level sensor	Level sensor shows zero (4mA)
F3	Bias failure of level sensor	Level sensor gets additional value (0.6mA)
F4	Noisy failure of level sensor	Level sensor gets more noise (Gaussian noise with zero mean and 0.2 variance)
F5	Partial failure of CWF sensor	CWF sensor gets stuck at the value of 7.5mA
F6	Total failure of CWF sensor	CWF sensors shows zero (4mA)
F7	Bias failure of CWF sensor	CWF sensor gets additional value (0.6mA)
F8	Noisy failure of CWF sensor	CWF sensor gets additional noise (Gaussian noise with zero mean and 0.2 variance)
F9	Partial failure of temperature sensor	Temperature sensor gets stuck at the value of 10.7mA
F10	Total failure of temperature sensor	Temperature sensors shows zero (4mA)
F11	Bias failure of temperature sensor	Temperature sensor gets additional value (0.6mA)
F12	Noisy failure of temperature sensor	Temperature sensor gets additional noise (Gaussian noise with zero mean and 0.2 variance)
F13	CW actuator failure	CW valve fails to close (gets stuck at the value of 8.3mA)
F14	Steam actuator failure	Steam valve fails to open (gets stuck at the value of 4mA)
F15	Disturbance failure	Step change in HW valve position to 6.5mA

The results for failures F1, F7, F9, F13, F14 and F15 are presented here.

For F1, as a failure scenario, the level sensor showed a constant value. While there is noise to cold water flow, it made the controller to go wrong and increased the cold water flow. The monitoring system tracked this abnormal condition. The level sensor stuck at t=1000s, the sensor output remained constant at the value of 11.99 mA, and the cold water flow started to increase.

Using Bank of Kalman Filter, the WSSR associated to each filter was calculated for which the results are shown in Figure 4-2. In this figure, the left plots are WSSR before filtering and the right ones are filtered WSSR. At time t=1074s the first Kalman filter, the filter used for identify failure in cold water flow sensor, deviated from the threshold. At this time the system knows that a failure has occurred in the plant. But, it is not able to diagnose the cause of failure till t=1260s at which all WSSR deviate from the threshold except one associated to level sensor identification. It is the time that the level sensor failure has detected and diagnosed. The delay in detecting time of failure is due to processing time.

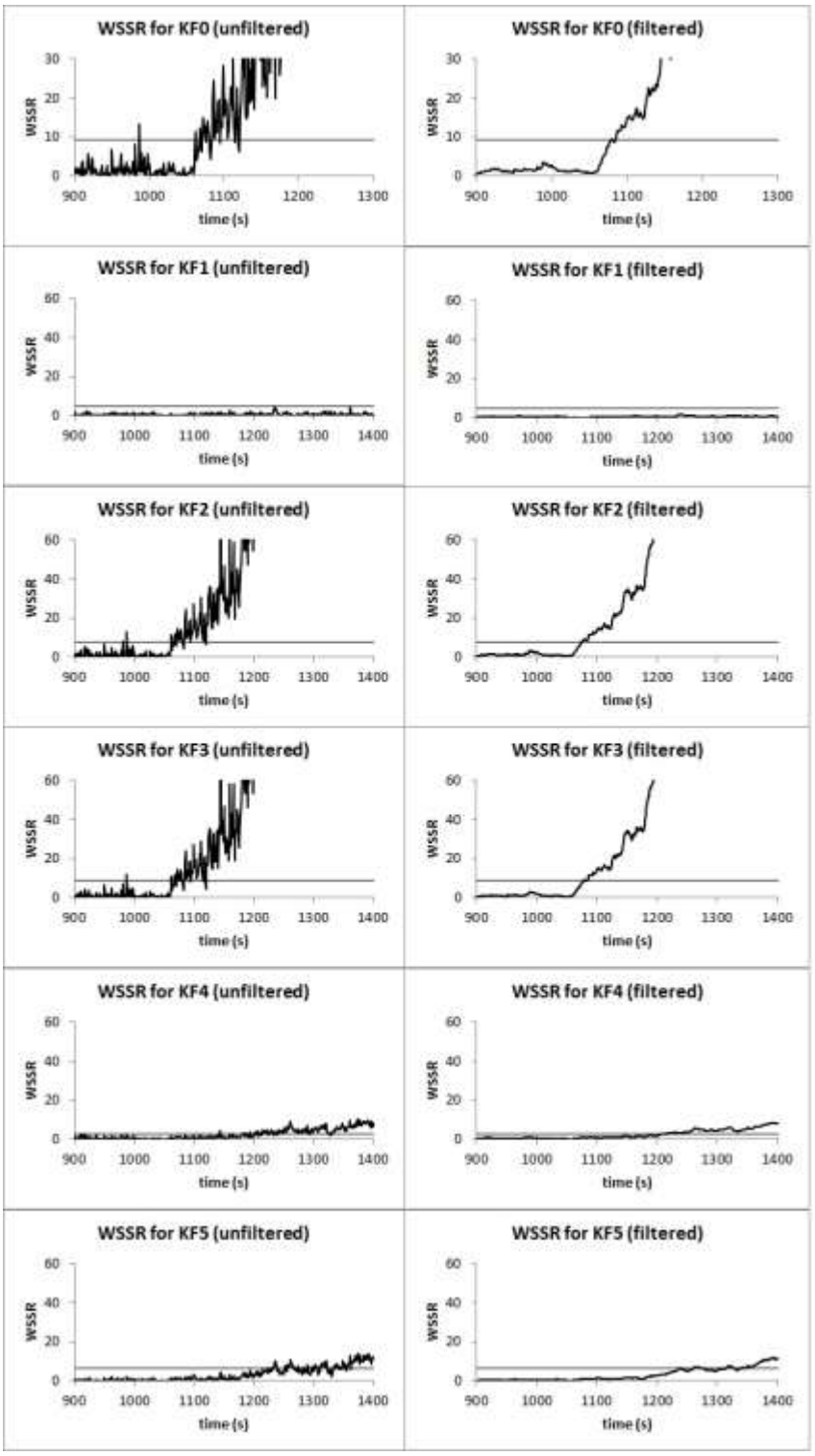

Figure 4-2: Fault indicators associated to 5 Kalman filters for failure F1; left plots are unfiltered and the right ones are filtered

In the bias failure of CWF sensor, failure F7, a constant value of 0.6 mA was added to the CWF sensor measurement at t=1000s. This affects the prediction accuracy of the model. The controller tries to reduce the CWF while affecting the level and the temperature of the tank. The fault indicator results for this failure scenario are shown in Figure 4-3. For this failure scenario, the first deviation happens at t=1003s when WSSR for KF3 exceeds the threshold and the fault is diagnosed at t=1028s when all WSSR cross their thresholds.

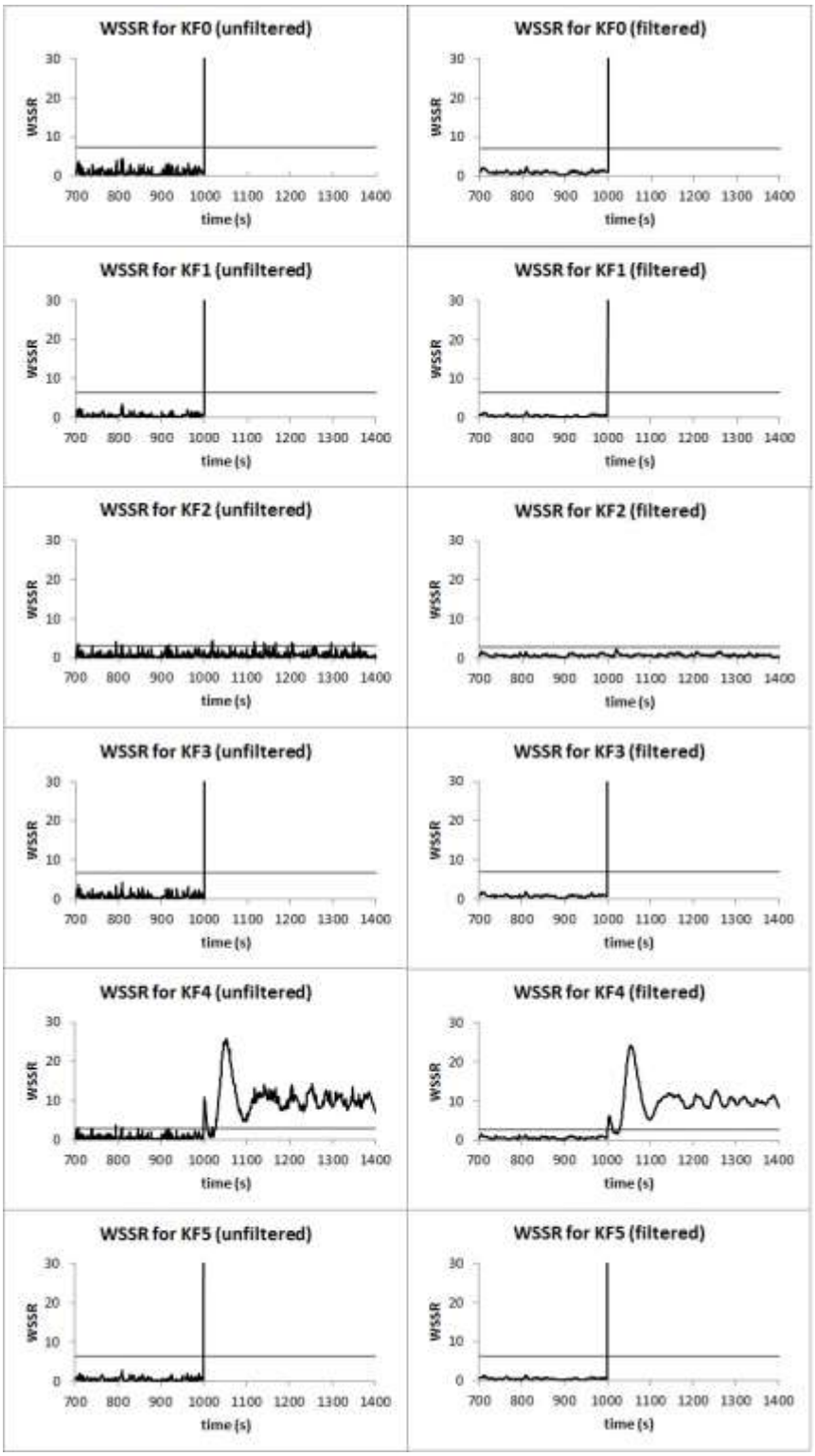

Figure 4-3: Fault indicators associated to 5 Kalman filters for failure F7; left plots are unfiltered and the right ones are filtered

In the next failure scenario, F9, the temperature sensor gets stuck at the value of 10.7 mA (the steady value of the operating point is 10.5 mA). The temperature controller tries to decrease the temperature by reducing the steam valve position. While the sensor value is wrong, it makes the real temperature of the tank to decrease. This failure does not affect the level of the tank. The results for fault indicators of this case are shown in Figure 4-4. The fault is detected at t=1000s when WSSR for KF4 exceeds the threshold and it's diagnosed at t=1056s.

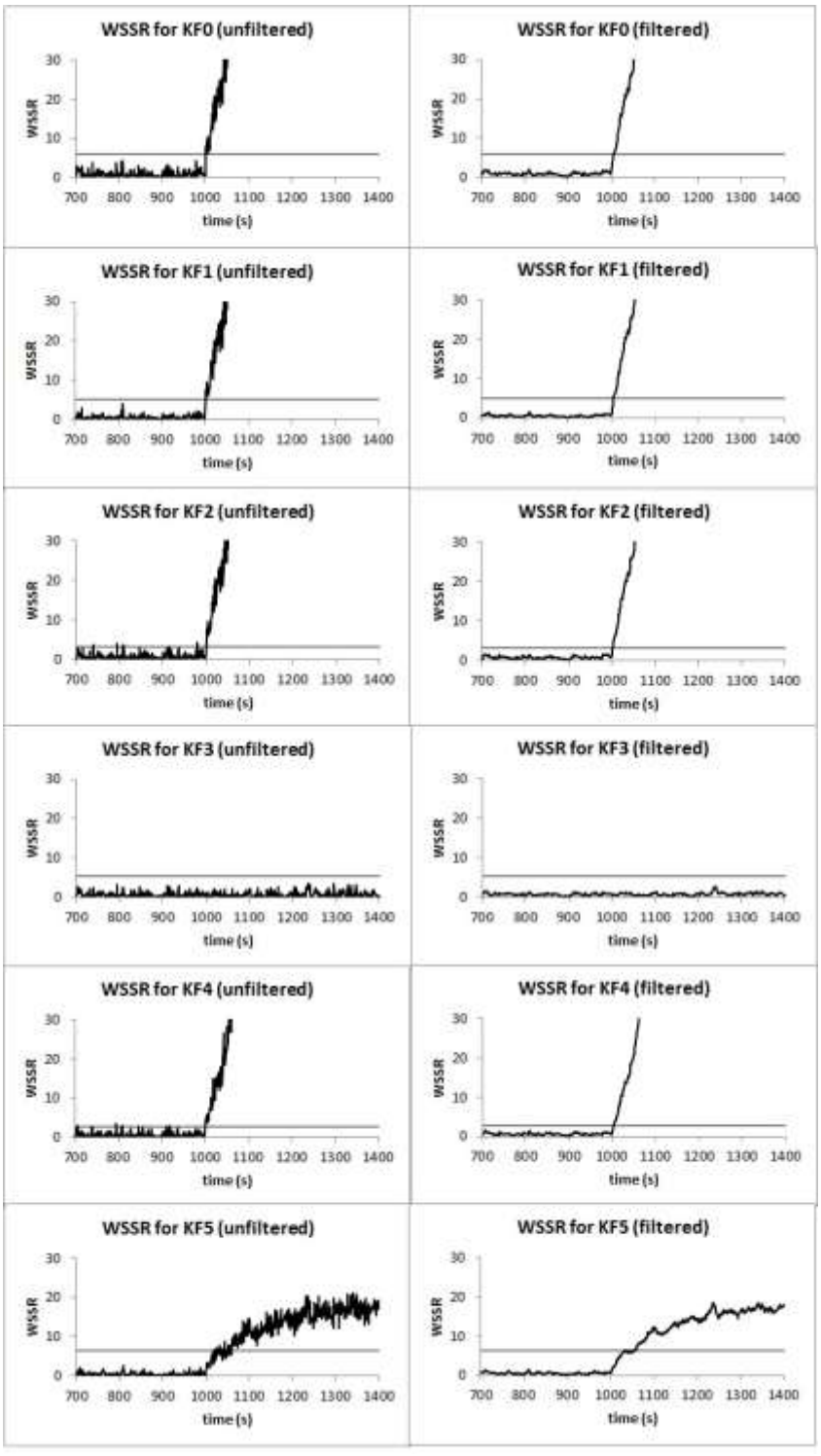

Figure 4-4: Fault indicators associated to 5 Kalman filters for failure F9; left plots are unfiltered and the right ones are filtered

In failure F13, as an actuator failure, the CW valve failed to close at t=1000s. In this scenario, the level set point and the temperature set point were changed in a pulse manner. The steady value for CW valve is 7.704 mA and as a failure it got stuck at the value of 8.3 mA. This change makes the CWF to increase and consequently the level of the tank increases. While the CW valve is stuck, the controller is unable to keep the level at the safe range, and finally tank overflow happens. Figure 4-5 shows the results for failure F13. The first fault indictor which detects the fault at t= 1002s is the one associated to KF1, but the CW actuator failure is diagnosed at t=1025s when all WSSR cross their thresholds.

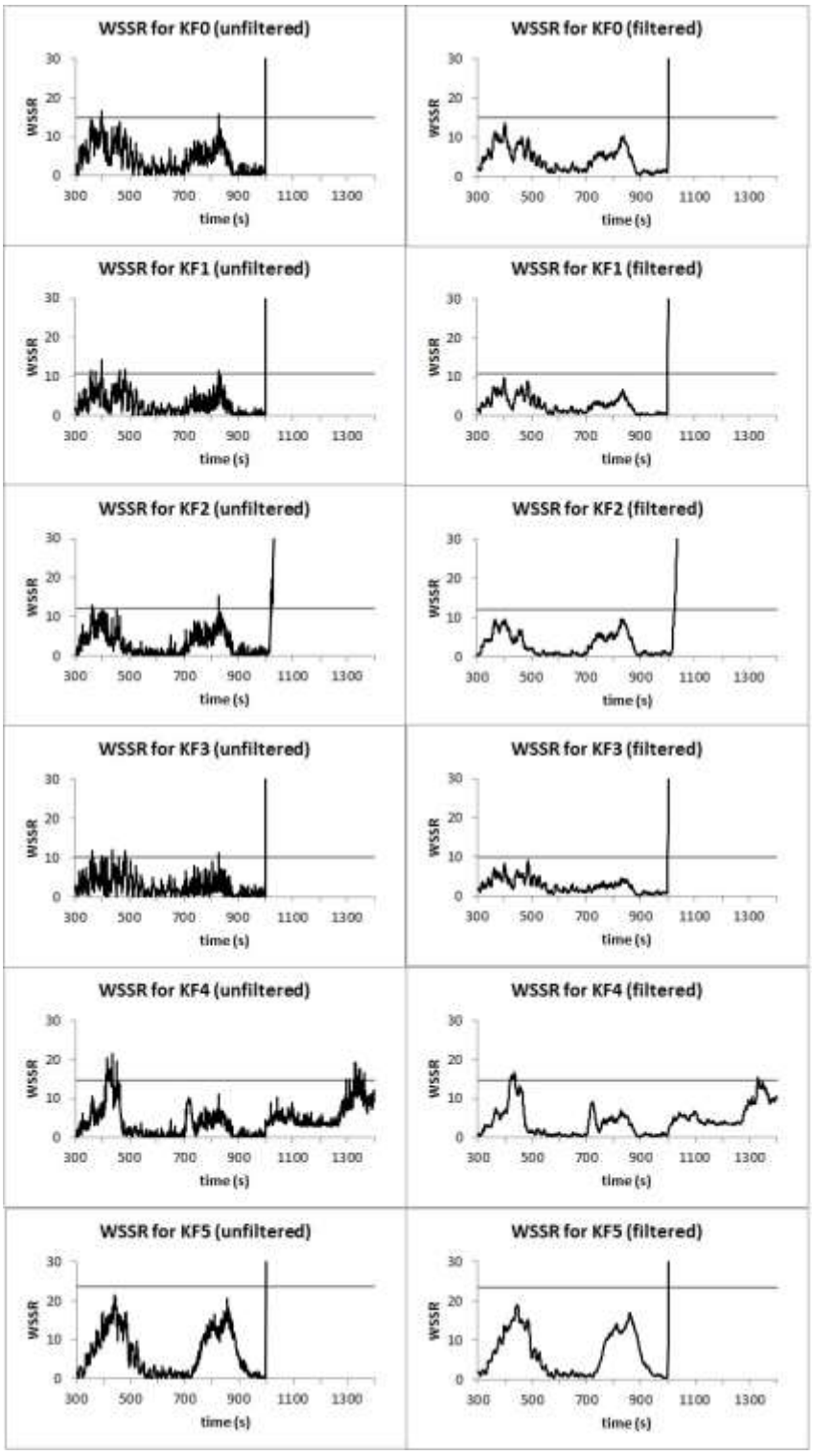

Figure 4-5: Fault indicators associated to 5 Kalman filters for failure F13; left plots are unfiltered and the right ones are filtered

Failure F14 represents another actuator failure. For this scenario, the level set point and the temperature set point were changed in a pulse manner. In this failure scenario, steam actuator fails to open. While this failure doesn't affect the level of the tank, it reduces the temperature of the tank, and the temperature controller is not able to fix it. Figure 4-6 represents the fault indicator results for failure F14. This failure is detected at t=1027s and its cause is diagnosed at t=1047s.

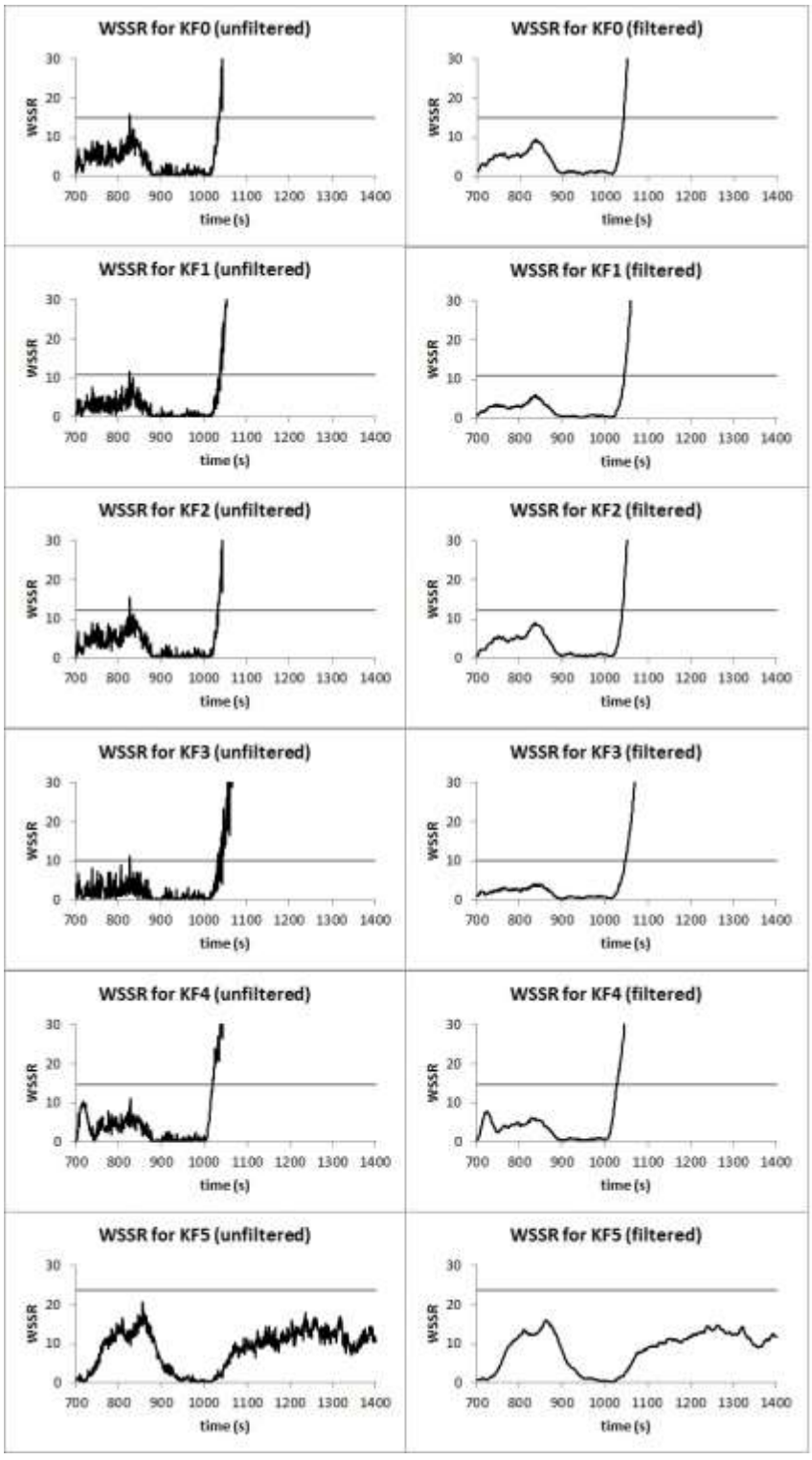

Figure 4-6: Fault indicators associated to 5 Kalman filters for failure F14; left plots are unfiltered and the right ones are filtered

As an example of disturbance failure, failure F15, HW got a step change from the steady value of 5.5 mA to 6.5 mA at t=1000s. Again, the level set point and the temperature set point were changed in a pulse manner. This affects both the level and the temperature of the tank. Level controller and temperature controller try to bring the system back to operating range by manipulating the CW and steam actuators. But the change is so big that the controllers can’t fix and it makes an increase in the level and the temperature of the tank. As shown in Figure 4-7, in the case of a disturbance failure, all fault indicators cross the threshold. This disturbance failure is detected at t=1011s when the first WSSR exceeds the threshold and at t=1014s all 5 fault indicators cross the limit.

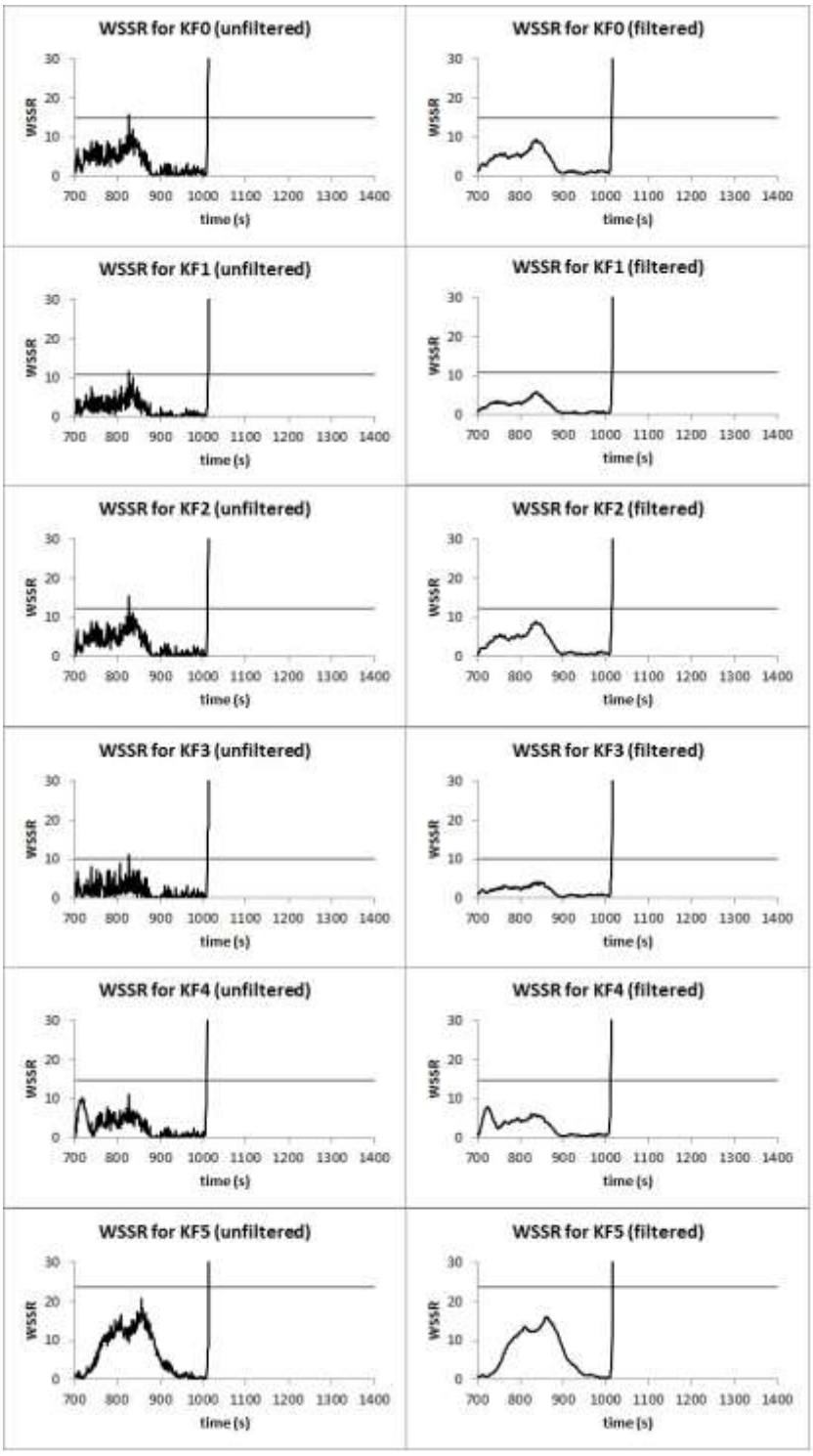

Figure 4-7: Fault indicators associated to 5 Kalman filters for failure F15; left plots are unfiltered and the right ones are filtered

4.1.2 Risk Quantification for CSTH

To find the risk profile, the probability of occurrence an event and its severity are needed to be calculated. The first step is finding the control failure probability to be applied to the event tree of the system.

Using Eq. (3-14) the probability of controller failure, the first barrier failure, is updated at each time. For hardware failure the fault indicator values of KF0 are used. The results for all failure scenarios are shown in Figure 4-8. At each time instant, the maximum value of WSSR is used to calculate the probability of the controller failure except in the case of disturbance failure in which the estimated states are used.

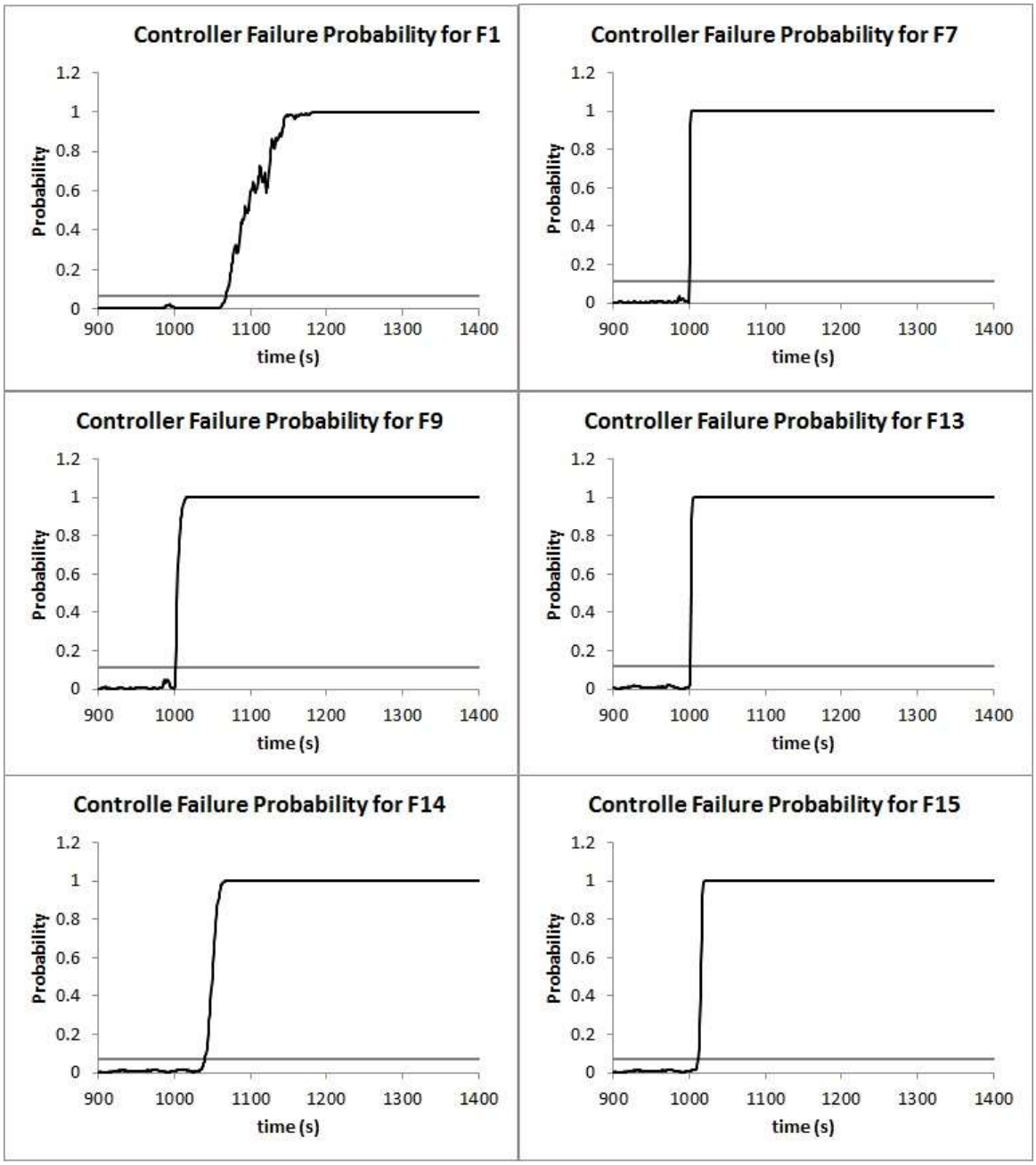

Figure 4-8: Controller failure probability for all failure scenarios for CSTH

Applying this updated probability to the event tree of the system, the updated probabilities of main outcomes are calculated. Figure 4-9 shows the Event Tree of the system in the case of failure F1. The numbers in the Event Tree are failure probabilities of each barrier (e.g. the failure probability of the Alarm System is 0.01), and F shows the failure probability of first barrier, control system, which is calculated at each time using the updated probability of the controller failure (Figure 4-8). For this failure, the outcomes are: safe, system shutdown and overflow of the system. Table 4-4 shows the outcomes for different failure scenarios.

Table 4-4: main outcomes for different failure scenarios for CSTH

Failure	Outcome
F1	Safe, System Shutdown, Overflow
F7	Safe, System Shutdown, Decrease in Level, Increase in Temperature
F9	Safe, System Shutdown, Decrease in Temperature
F13	Safe, System Shutdown, Overflow
F14	Safe, System Shutdown, Decrease in Temperature
F15	Safe, System Shutdown, Overflow, Increase in Temperature

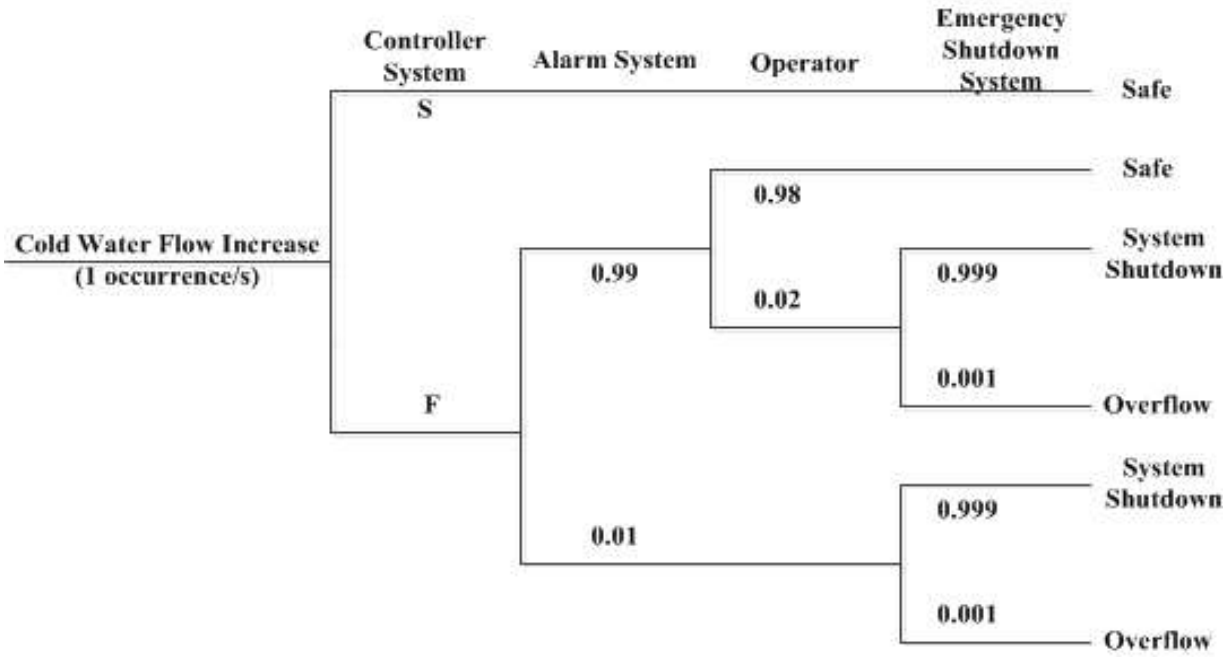

Figure 4-9: Event Tree of the CSTH system in case of F1

The updated probabilities of the main outcomes in different failure scenarios are shown in Figure 4-10. As is shown in this figure, one barrier failure increases the probability of main outcomes.

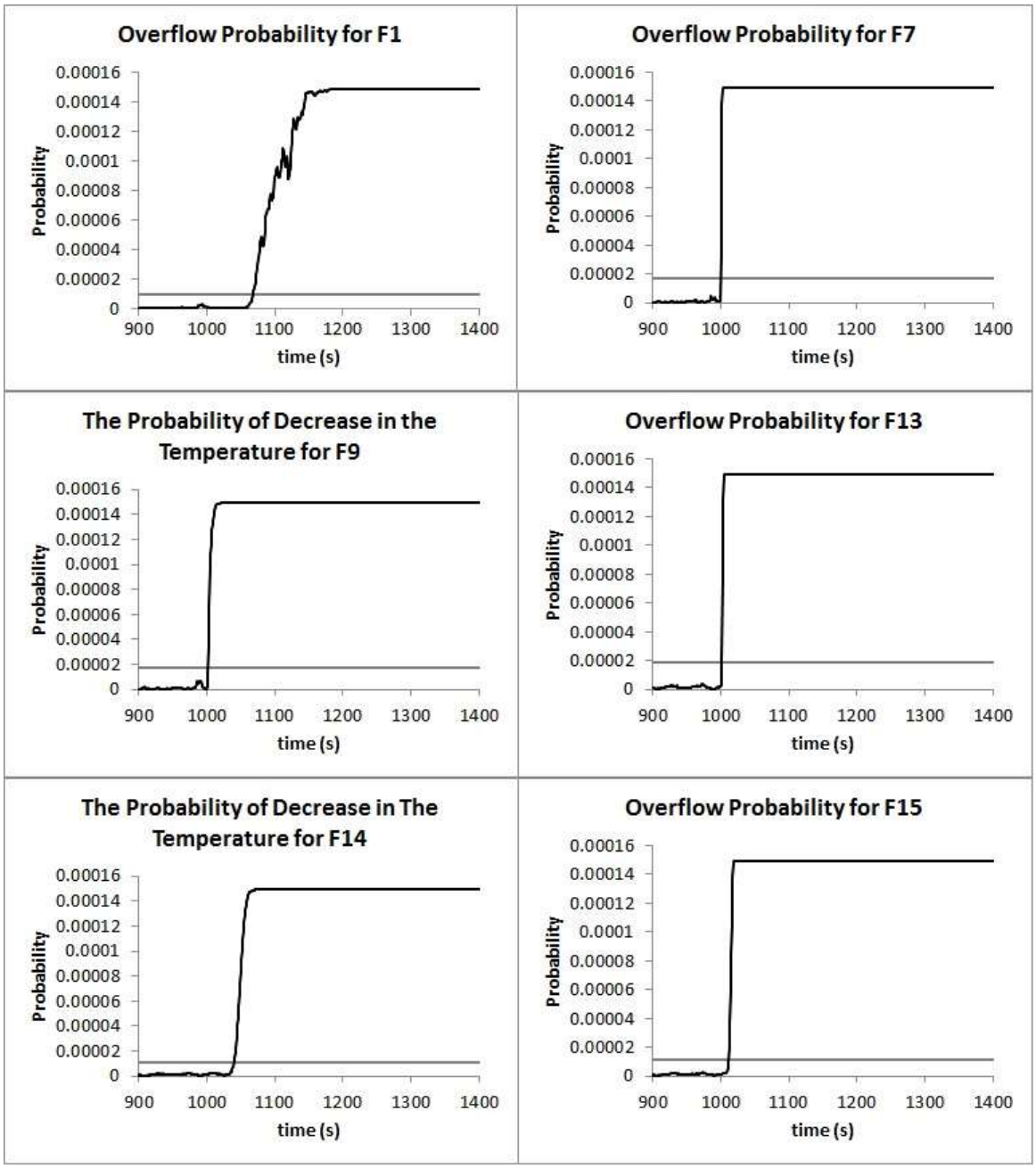

Figure 4-10: The Probability of the occurrence of the main outcomes in different failure scenarios for CSTH

The severity of the failure is calculated using Eq. (3-15), Figure 4-11, and the risk of the system operating under faulty conditions is updated using Eq. (3-13), for which the results of different failure scenarios are shown in Figure 4-12.

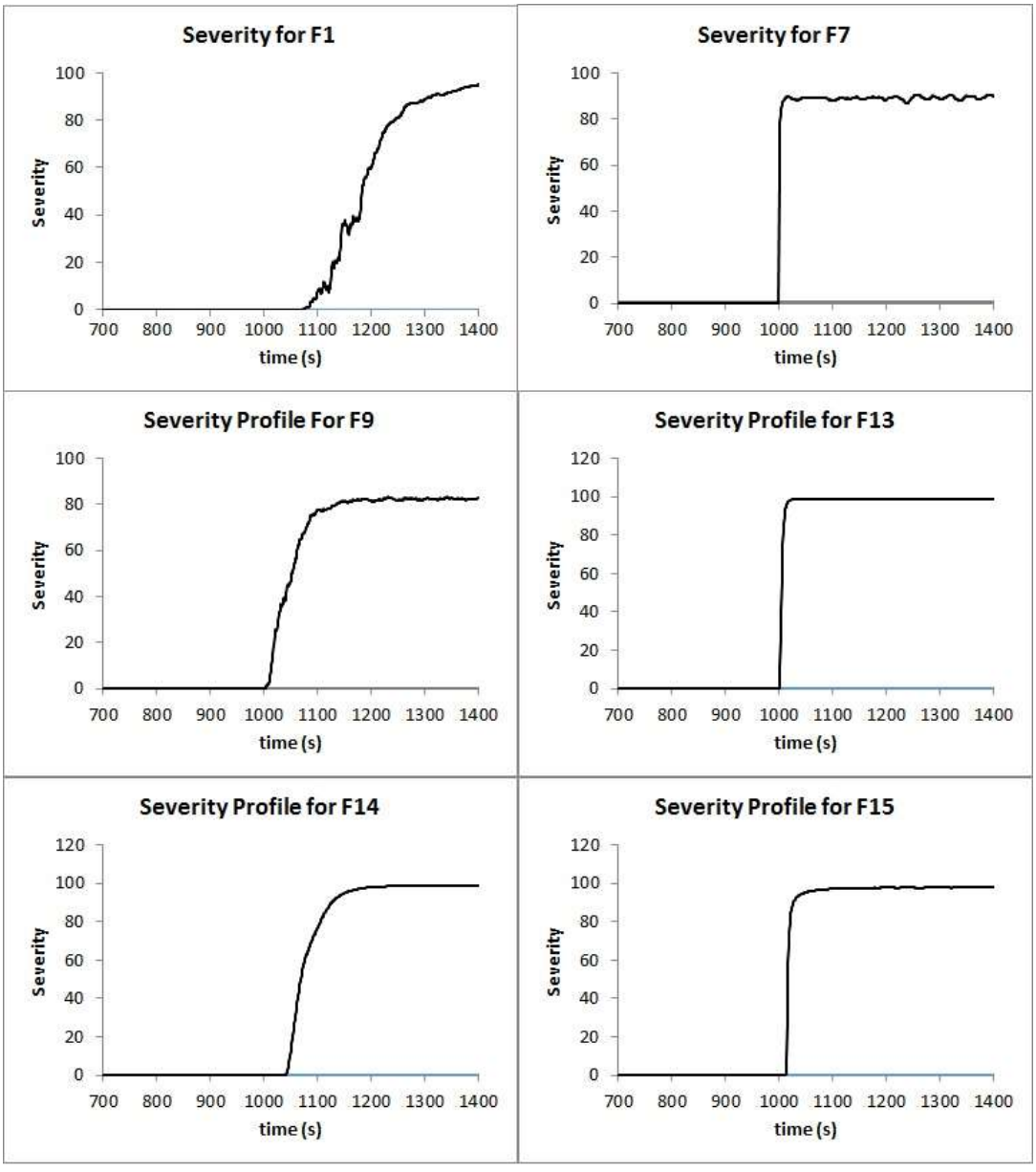

Figure 4-11: Severity profile for different failure scenarios for CSTH

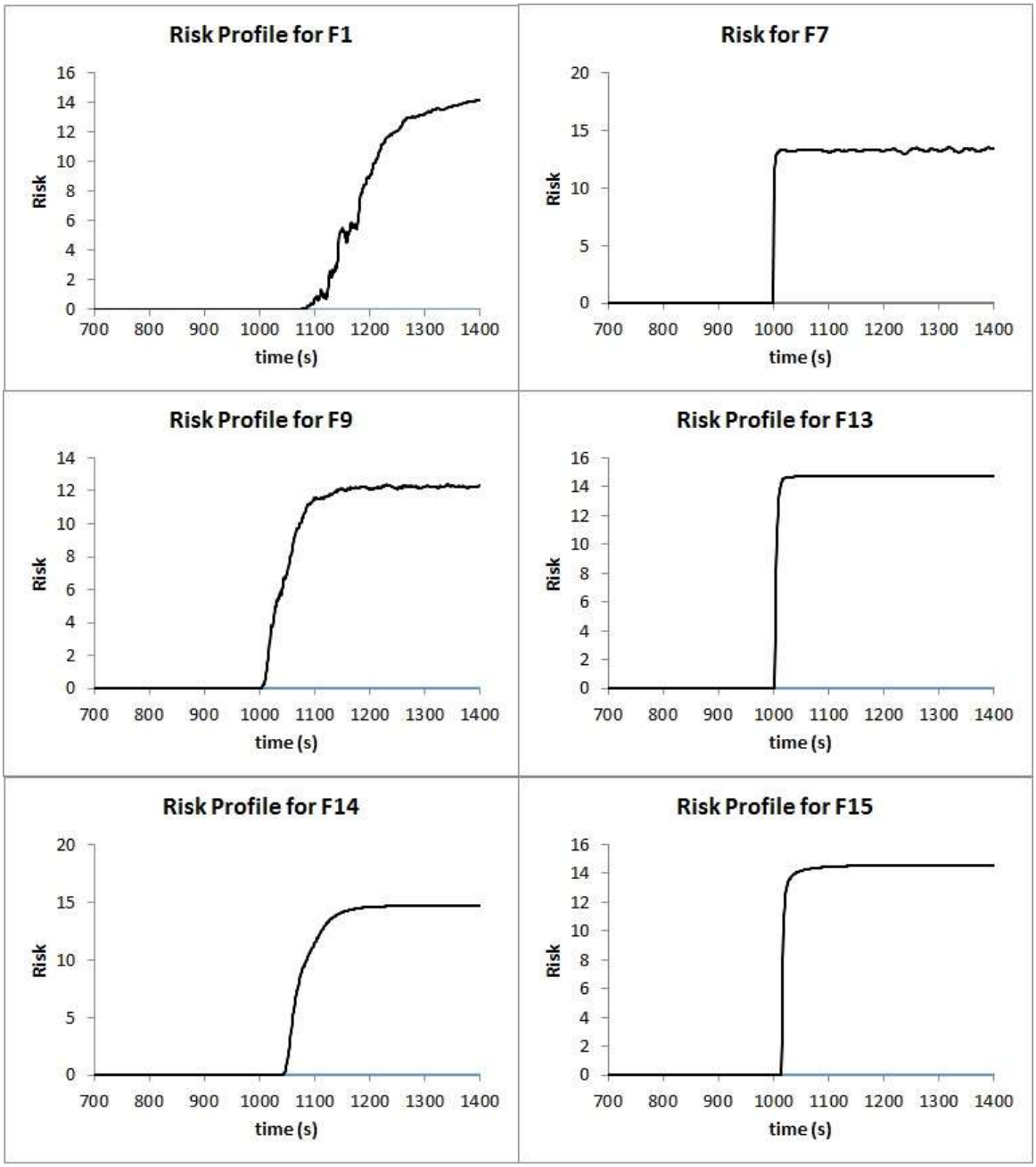

Figure 4-12: Risk profile for different failure scenarios for CSTH

Table 4-5 summarizes the results for fault detection and diagnosis and the risk for all failure scenarios. As seen from this table, in most cases, using the risk, the fault is detected at an earlier time:

- F1: fault indicators detect the fault at t=1074s, the risk profile detects the fault at t=1069s,
- F7: fault indicators detect the fault at t=1003s, the risk profile detects the fault at t=1001s,
- F9: fault indicators detect the fault at t=1003s, the risk profile detects the fault at t=1002s,
- F13: fault indicators detect the fault at t=1002s, the risk profile detects the fault at t=1002s,
- F14: fault indicators detect the fault at t=1027s, the risk profile detects the fault at t=1025s, and
- F15: fault indicators detect the fault at t=1011s, the risk profile detects the fault at t=1010s,

Table 4-5: deviation time of each fault indicator and the risk profile from the threshold for CSTH

Failure	WSSR1	WSSR2	WSSR3	WSSR4	WSSR5	R
F1	-	1074	1077	1214	1260	1069
F7	1005	-	1003	1028	1006	1001
F9	1008	1004	-	1003	1056	1002
F13	1002	1025	1003	-	1003	1002
F14	1044	1040	1047	1027	-	1025
F15	1014	1013	1013	1011	1014	1010

4.2 RT 580

The RT 580 fault finding in control systems setup (Figure 4-13) located in CRISE (Centre for Risk, Integrity and Safety Engineering) at Memorial University of Newfoundland was used to demonstrate the proposed methodology. RT 580 has 5 different control systems: level control system, flow control system, temperature control system, level-flow cascade control system and flow-temperature cascade control system.

Figure 4-13: RT 580 fault finding in control systems setup

The methodology is applied to level control system. The schematic diagram of the plant is shown in Figure 4-14. In the experimental setup, water from the collecting (reservoir) tank is pumped to a process tank and from there goes back to the reservoir tank. The aim

of level control system is to control the level of the process tank using a controller to manipulate the inlet flow to the process tank. To find the relevant matrices of the continuous state space model of the system, Eq. (4-1), open loop system identification experiment was done by changing the inlet valve position in a stepwise manner and measuring the flow and the level of the process tank. For experimental scenario, Eq. (4-1) has one input, the control valve position, and two outputs, the level of the process tank and the inlet flow to the tank.

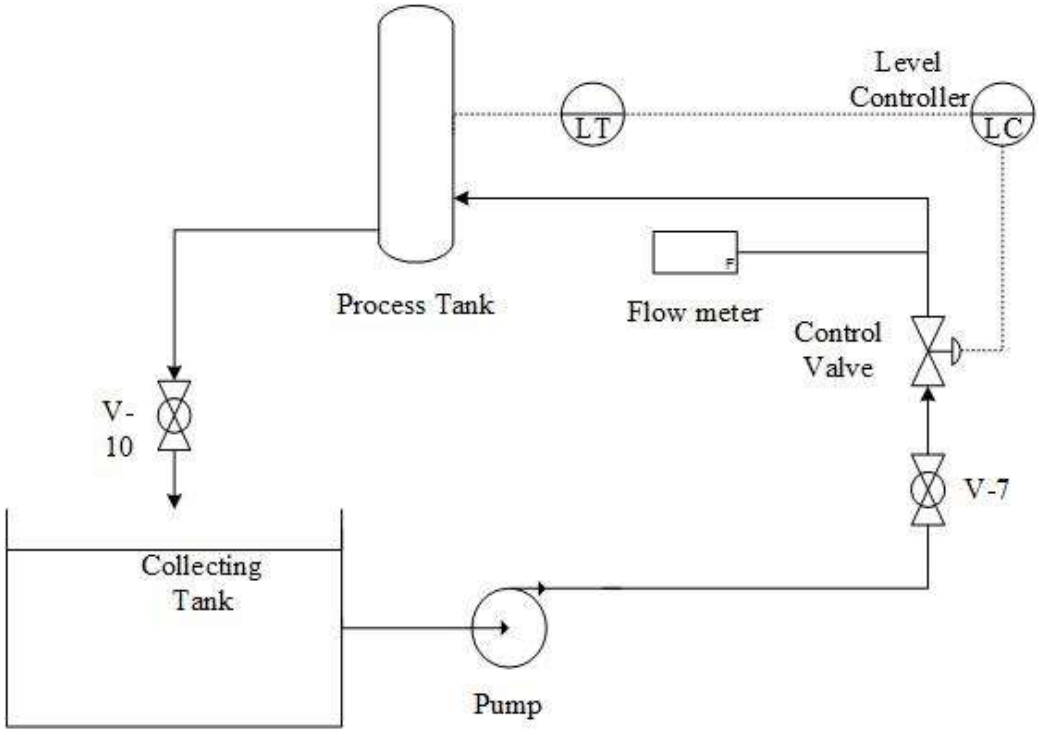

Figure 4-14: Schematic diagram of the RT 580 setup

Figure 4-15 shows the step test data for the open loop experiments.

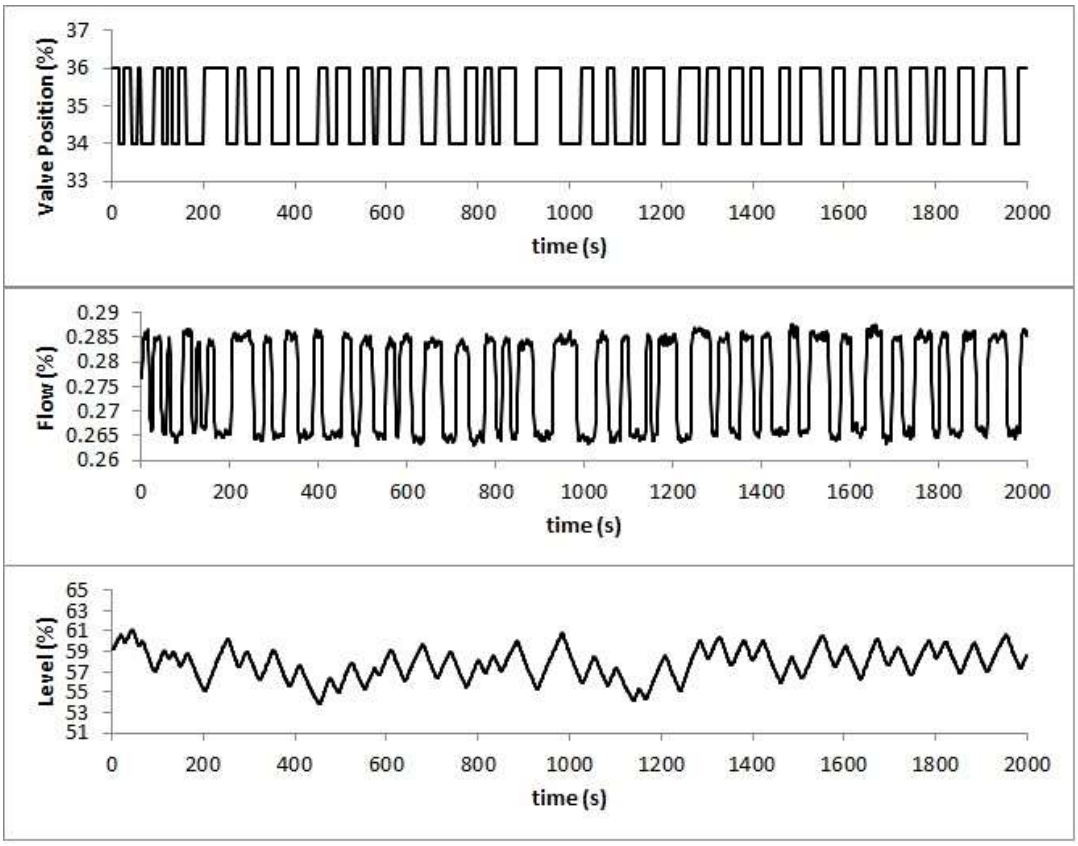

Figure 4-15: Step test data for open loop experiment: valve position (top), flow (middle) and level (bottom)

Using System Identification Toolbox of MATLAB, the matrixes A, B and C in Eq. (4-1) for RT 580 are found as:

$$A=\begin{bmatrix} 0.2488 & 0.2222 & 0.1259 \\ -2.307 & 2.708 & -5.529 \\ 1.157 & 11.88 & -10.61 \end{bmatrix}, \quad B=\begin{bmatrix} -0.008781 \\ -0.4275 \\ -3.22 \end{bmatrix}, \quad C=\begin{bmatrix} 11.77 & 0.4767 & -0.1479 \\ 2.516 & 2.698 & -0.3204 \end{bmatrix}$$

Three fault scenarios were simulated in the system: F1: level sensor failure, F2: actuator failure and F3: disturbance fault by changing the cock-boll valve V-7. Subsequently, four Kalman filters were designed: KF0 with the hypothesis that the system works with no

fault, KF1 for detecting and diagnosing level sensor failure, KF2 for flow sensor failure and KF3 for actuator failure.

In the first failure, level sensor fails at t=350s, the sensor fails to the lowest value, which makes the control command to increase the valve position. As seen in Figure 4-16, fault indicators for KF0, KF2 and KF3 increase after the fault happens in the system, but fault indicator for KF1 stays in the normal range. It means the fault in the system is the one associated with KF1, level sensor failure.

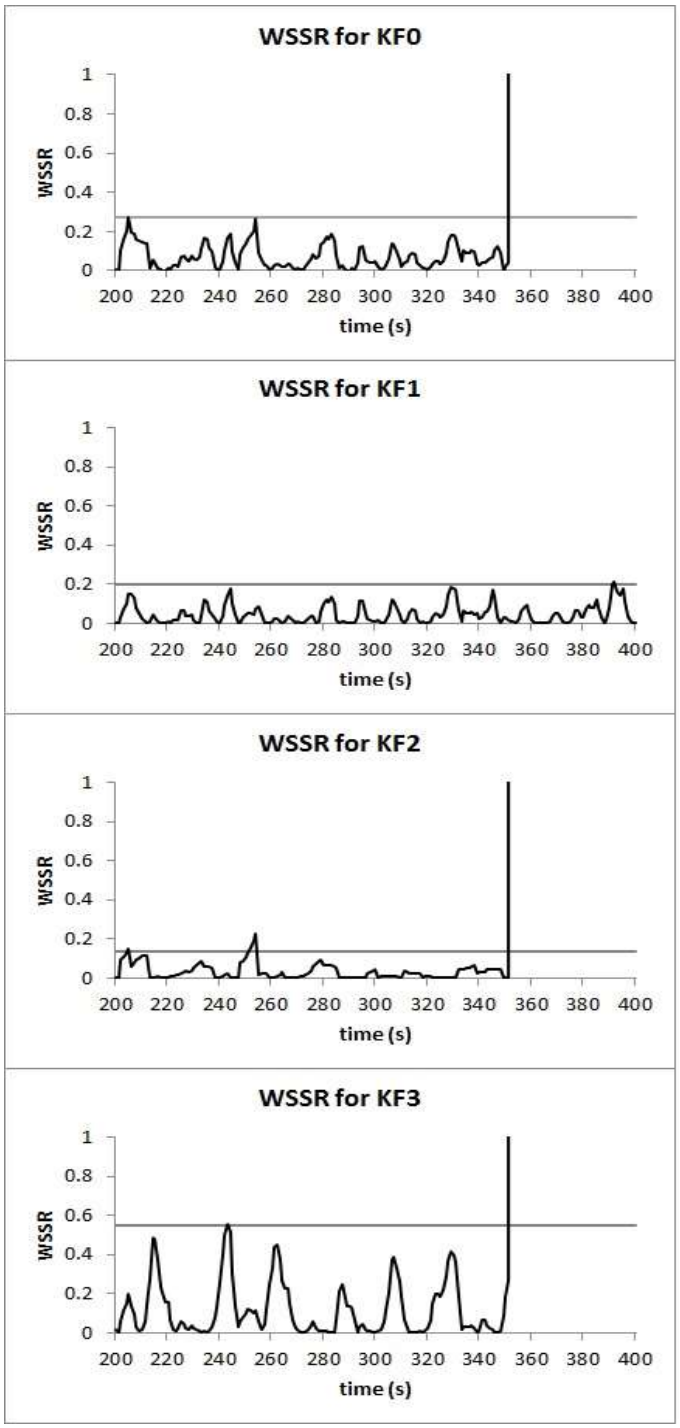

Figure 4-16: Fault indicators for 4 Kalman filters in the case of sensor failure for RT 580

In the second failure, as an example of actuator failure, the control valve fails to open at t=350s. For this case, Figure 4-17, the fault indicators associated to KF0, KF1 and KF2 increase after the fault occurs which means the fault is diagnosed as the actuator failure identified by KF3.

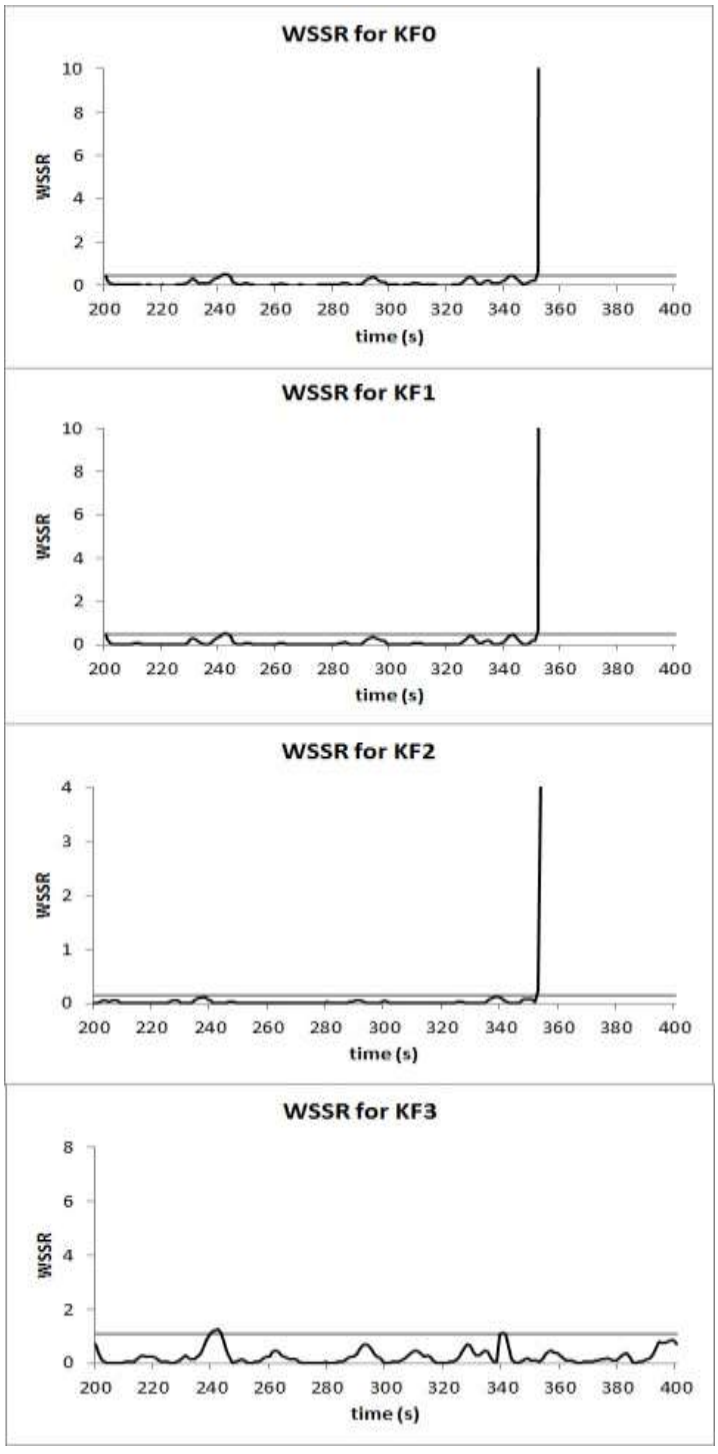

Figure 4-17: Fault indicators for 4 Kalman filters in the case of actuator failure for RT 580

To simulate disturbance failure, the opening of cock-boll valve V-7 was reduced at t=260s. This change made the flow to decrease which lead to reduction in the level of the process tank. As seen in the Figure 4-18, for this failure, all fault indicators increased. So, a fault is detected in the system, but the cause of the failure cannot be identified.

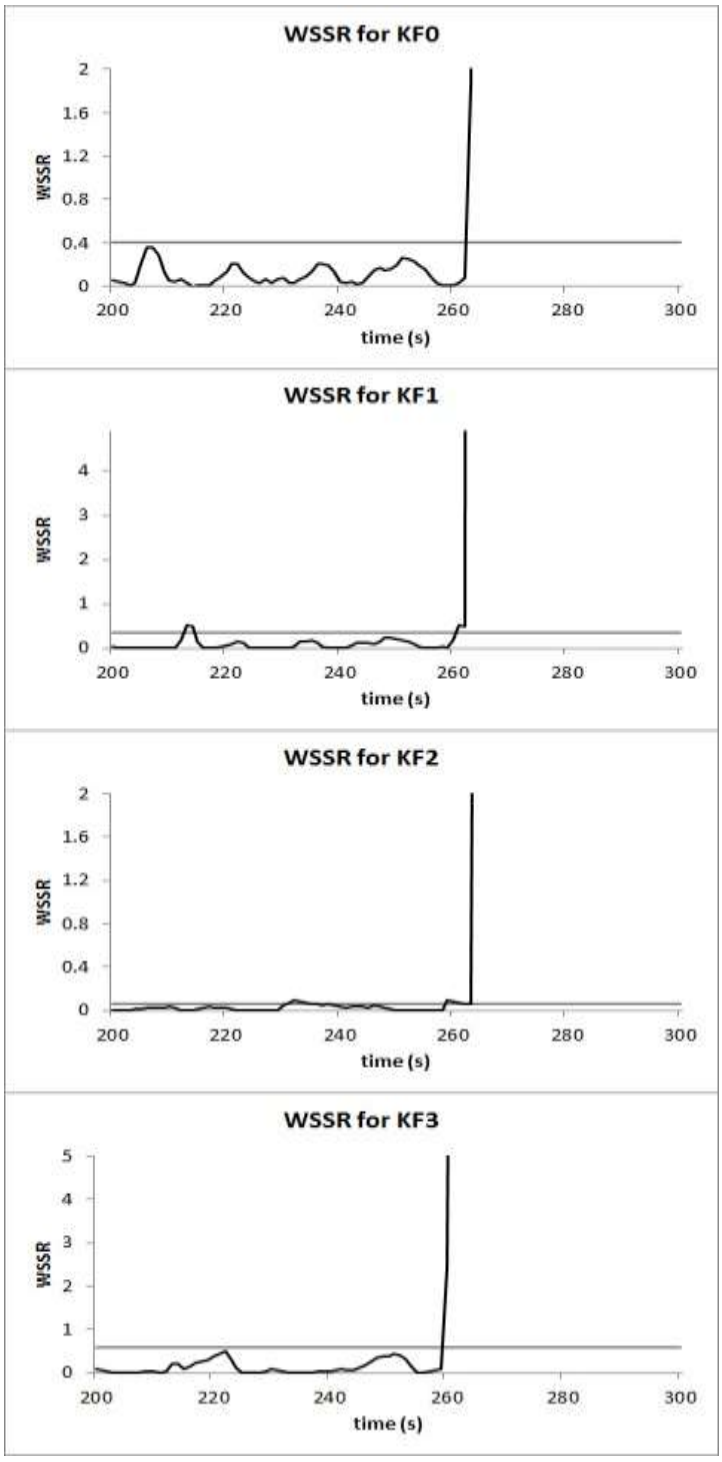

Figure 4-18: Fault indicators for 4 Kalman filters in the case of disturbance failure for RT 580

At each time instant, the probability of failure of the controller system, first barrier in the event tree of the system, is updated using Eq. (3-14) for which the results are shown in Figure 4-19.

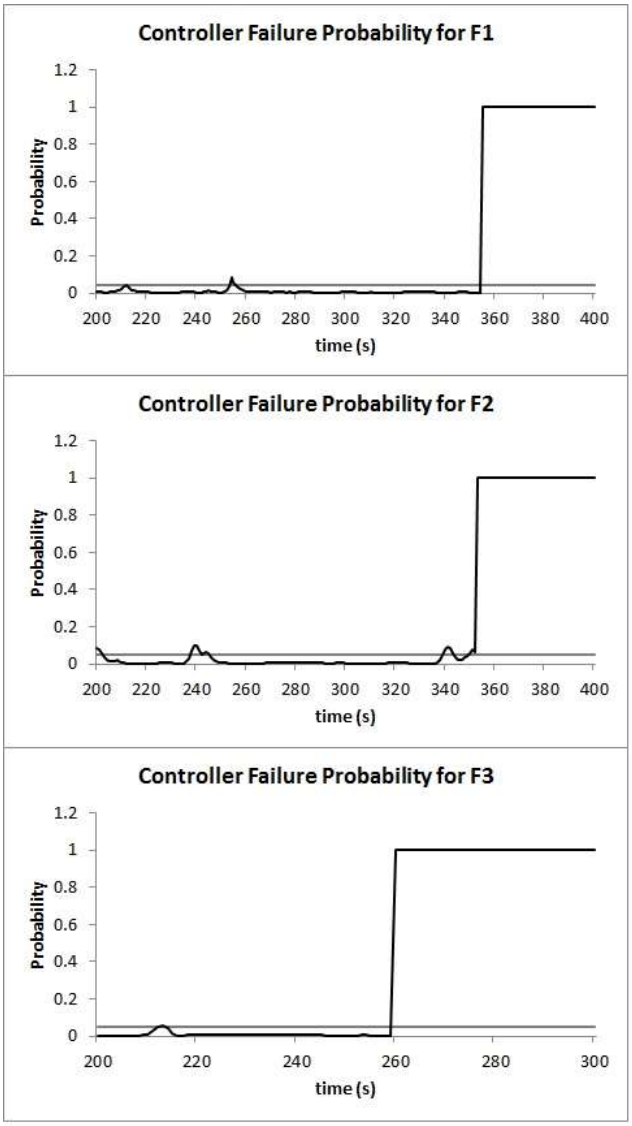

Figure 4-19: controller failure probability for 3 failure scenario for RT 580

The controller failure probability is applied to the event tree of the system which is shown in Figure 4-20. The numbers in the Event Tree are failure probabilities of each barrier (e.g. the failure probability of the Emergency Shutdown System is 0.001), and F shows the failure probability of the first barrier, control system. Applying this probability to the event tree of the system, the probability of the outcome, the process tank goes dry, is calculated for which the results are shown in Figure 4-21. As is shown in this figure, the failure of one barrier increases the probability of catastrophic outcomes, decrease in the system level.

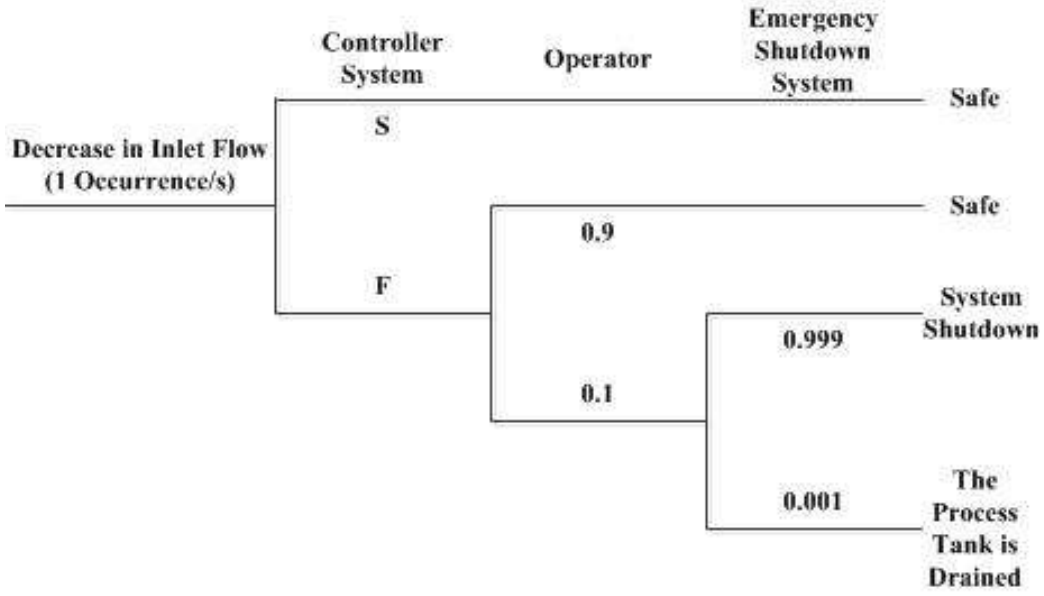

Figure 4-20: Event tree for level control setup of RT 580

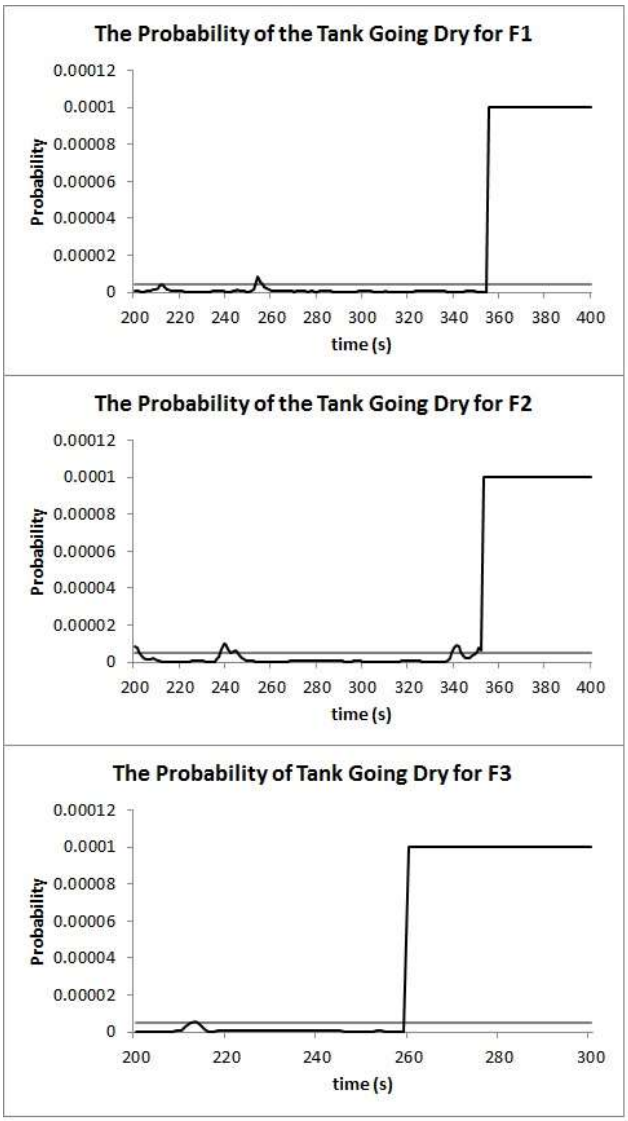

Figure 4-21: The Probability of the system goes dry for 3 failure scenarios for RT580

The severity and the risk of the failure are calculated using Eq. (3-15) and Eq. (3-13).

Figures 4-22 and 4-23 show the results for severity and the risk, respectively.

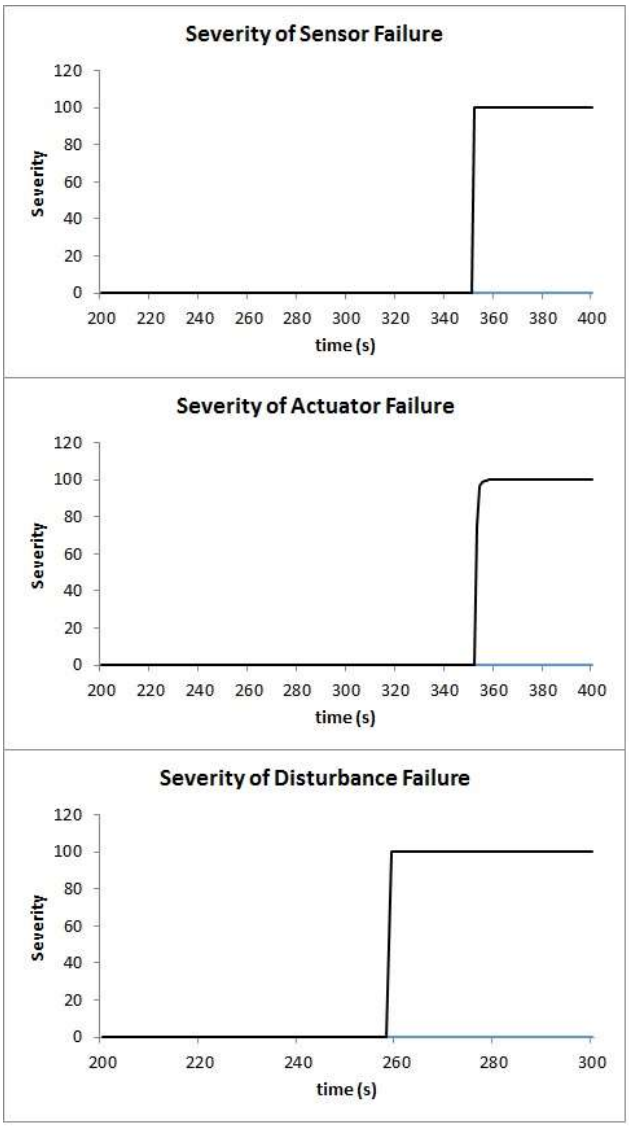

Figure 4-22: severity profile for 3 failure scenarios for RT580

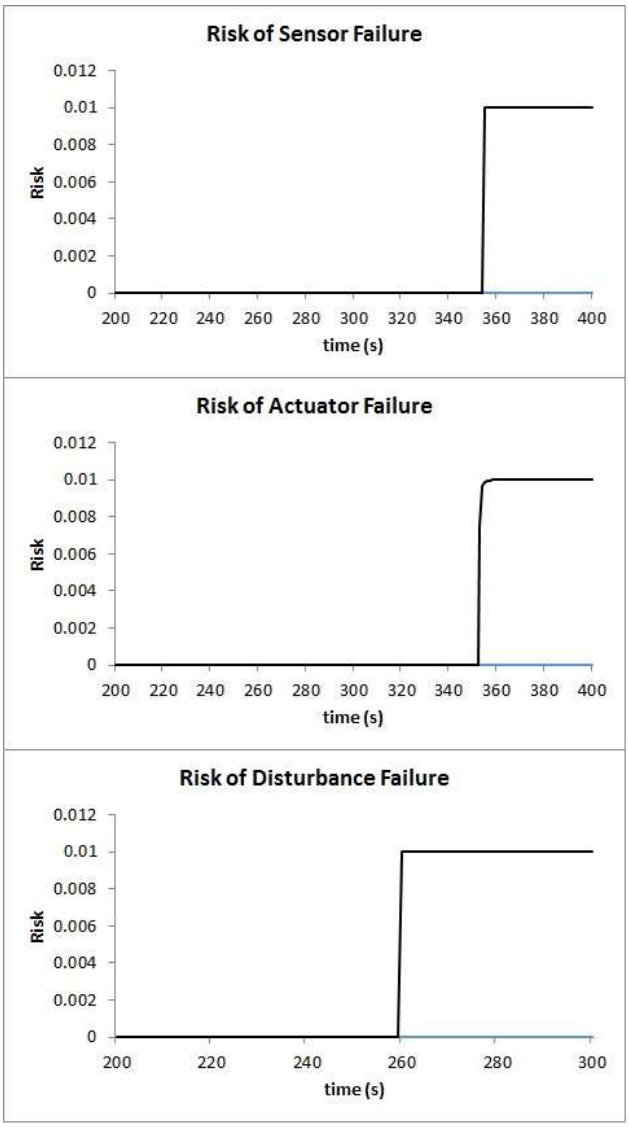

Figure 4-23: Risk profile for 3 failure scenarios for RT580

4.3 Summary

The proposed methodology was applied to two case studies. First example was CSTH for which the state space model was used. For this example, there are 15 possible failure scenarios of which some results are provided in this chapter. For each failure scenario, the

fault was correctly detected and diagnosed. After classifying the faults, the risk of model operating under different conditions were calculated. The results showed that using risk as a fault detector, the operators would have more time to take action in case of an unwanted event.

The methodology was also applied to an experimental set up, RT 580 fault finding in control systems. The experimental results showed correct detection and diagnosis for different types of failures.

5 CONCLUSION AND FUTURE WORK

5.1 Concluding Remarks

In this study, a new methodology is proposed for online risk assessment using a combination of Bank of Kalman Filters and Event Tree Analysis. The proposed methodology uses two sets of Bank of Kalman Filters to detect and diagnose sensor and actuator faults. Each filter is designed to detect and diagnose the failure in one single sensor or one single actuator. In case of a fault, all fault indicators associated to Kalamn Filters deviate from a threshold except one which is designed for the faulty part. The methodology was able to detect and diagnose different sensor faults and actuator faults. It also detects disturbance fault. Here, different types of failures are classified and the risk for different types of failures are calculated. Using residuals obtained from Kalman Filters, the probability and severity of failure is updated at each time. Applying these updated probabilities to Event Tree, the probability of catastrophic event is updated. Using these updated probabilities, the risk of the system operating under faulty conditions is assessed online. The method has several advantages: (i) it is able to distinguish between different types of failures, (ii) it provides an alarm early to notify the operator that there is failure in the system and diagnosed the cause, (iii) Using Event Tree, the safety of the current system is investigated, and if it is necessary, additional barriers are added to the system to improve the safety.

5.2 Future Work

As an assumption in this study, at each time only one fault occurs in the system. The methodology needs to be modified to be able to detect and diagnose multiple faults at the same time. The modification can be done by improving the ability of fault indicators to detect multiple failures at the same time.

Here a bank of Kalman filters were used to detect and diagnose different types of failure for linear time invariant models. In case of nonlinear and/or time variant models other types of filters such as particle filter can be used.

The results need to be compared to some available methods.

6 REFERENCES

Ahmed, S., Gabbar, H. A., Chang, Y., & Khan, F. I. (2011, May). Risk based alarm design: A systems approach. In Advanced Control of Industrial Processes (ADCONIP), 2011 International Symposium on (pp. 42-47). IEEE.

Argiolas, C., Carbonari, A., Melis, F., & Quaquero, E. (2012). A Bayesian model for real-time safety management in construction sites. Gerontechnology, 11(2), 149.

Bao, H., Khan, F., Iqbal, T., & Chang, Y. (2011). "Risk-based fault diagnosis and safety management for process systems". Process Safety Progress,30(1), 6-17.

Barnett, L., Barrett, A. B., & Seth, A. K. (2009). Granger causality and transfer entropy are equivalent for Gaussian variables. Physical review letters, 103(23), 238701.

Bauer, M., Cox, J. W., Caveness, M. H., Downs, J. J., & Thornhill, N. F. (2007). Finding the direction of disturbance propagation in a chemical process using transfer entropy. IEEE transactions on control systems technology, 15(1), 12-21.

Bouhouche, S., Lahreche, M., Ziani, S., & Bast, J. (2005, November). "Fault detection and monitoring of length loop control system in pickling process". In Computational Intelligence for Modelling, Control and Automation, 2005 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, International Conference on (Vol. 1, pp. 642-647). IEEE.

Chiang, L. H., Braatz, R. D., & Russel, E. L. (2001). "Fault Detection and Diagnosis in Industrial Systems", Springer Science & Business Media.

Cochran, E. L., Miller, C., & Bullemer, P. (1996, May). Abnormal Situation Management in petrochemical plants: can a Pilot's Associate crack crude?. In Aerospace and Electronics Conference, 1996. NAECON 1996., Proceedings of the IEEE 1996 National (Vol. 2, pp. 806-813). IEEE.

Crowl, D. A., & Louvar, J. F. (2001). "Chemical process safety: fundamentals with applications". Pearson Education.

Dalaptadu, K. P. S. (2014). “Design of an event-based early warning system for process operations”, (Doctoral dissertation, Memorial University of Newfoundland).

Ding, S. (2008). Model-based fault diagnosis techniques: design schemes, algorithms, and tools. Springer Science & Business Media.

EEMUA. (2007). Alarm Systems, a guide to design, management and procurement, Publication No 191 (2nd ed.). The Engineering Equipment and Materials Users Association publication.

Ferdous, C. M. R. (2011). “Quantitative Risk Analysis in an Uncertain and Dynamic Environment”, (Doctoral dissertation, Memorial University of Newfoundland).

Hlaváčková-Schindler, K., Paluš, M., Vejmelka, M., & Bhattacharya, J. (2007). Causality detection based on information-theoretic approaches in time series analysis. Physics Reports, 441(1), 1-46.

Hollender, M., & Beuthel, C. (2007). Intelligent alarming. ABB review, 1, 20-23.

Hossain, M., & Muromachi, Y. (2012). A Bayesian network based framework for real-time crash prediction on the basic freeway segments of urban expressways. Accident Analysis & Prevention, 45, 373-381.

Hotz, I., Hanisch, A., & Schulze, T. (2006, December). Simulation-based early warning systems as a practical approach for the automotive industry. In Proceedings of the 38th conference on Winter simulation (pp. 1962-1970). Winter Simulation Conference.

Hsoumi, A., Harabi, R. E., Ali, S. B. H., & Abdelkrim, M. N. (2009, September). “Diagnosis of a Continous Stirred Tank Reactor Using Kalman Filter”. In Computational Intelligence, Modelling and Simulation, 2009. CSSim'09. International Conference on (pp. 153-158). IEEE.

International Society of Automation (ISA), ANSI/ISA-18.2-2009, Management of alarm systems for the process industries, 2009.

Ishtiaque, S., Jabeen, S., & Shoukat, S. (2017). Hazop Study on Oil Refinery Waste Water Treatment Plant in Karachi.

Izadi, I., Shah, S. L., Shook, D. S., Kondaveeti, S. R., & Chen, T. (2009a). A framework for optimal design of alarm systems. IFAC Proceedings Volumes, 42(8), 651-656.

Izadi, I., Shah, S. L., Shook, D. S., & Chen, T. (2009b). An introduction to alarm analysis and design. IFAC Proceedings Volumes, 42(8), 645-650.

Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., & Mannan, M. S. (2018). Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. Journal of Loss Prevention in the Process Industries, 53, 61-73.

Kang, H. G., & Seong, P. H. (1999). A methodology for evaluating alarm-processing systems using informational entropy-based measure and the analytic hierarchy process. IEEE Transactions on Nuclear Science, 46(6), 2269-2280.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliability Engineering & System Safety, 96(8), 925-932.

Kobayashi, T., & Simon, D. L. (2004, January). "Evaluation of an enhanced bank of Kalman filters for in-flight aircraft engine sensor fault diagnostics". In ASME Turbo Expo 2004: Power for Land, Sea, and Air (pp. 635-645). American Society of Mechanical Engineers.

Kondaveeti, S. R., Shah, S. L., & Izadi, I. (2009). Application of multivariate statistics for efficient alarm generation. IFAC Proceedings Volumes, 42(8), 657-662.

Kondaveeti, S. R., Izadi, I., Shah, S. L., & Black, T. (2010). Graphical representation of industrial alarm data. IFAC Proceedings Volumes, 43(13), 181-186.

Li, W., Shah, S. L., & Xiao, D. (2008). "Kalman filters in non-uniformly sampled multirate systems: for FDI and beyond". Automatica, 44(1), 199-208.

Lu, C. Y., Simon, G., Soumerai, S. B., & Kulldorff, M. (2018). Counter-point: Early Warning Systems Are Imperfect, but Essential. Medical care, 56(5), 382-383.

Noda, M., Higuchi, F., Takai, T., & Nishitani, H. (2011). Event correlation analysis for alarm system rationalization. Asia-Pacific Journal of Chemical Engineering, 6(3), 497-502.

Ora, A., Nandan, A., & Kumar, A. (2017). Hazard Identification of Chemical Mixing Plant through Hazop Study. International Journal for Advance Research and Development, 2(3).

Rago, C., Prasanth, R., Mehra, R. K., & Fortenbaugh, R. (1998, December). Failure detection and identification and fault tolerant control using the IMM-KF with applications to the Eagle-Eye UAV. In Decision and Control, 1998. Proceedings of the 37th IEEE Conference on (Vol. 4, pp. 4208-4213). IEEE.

"risk, n." OED Online. Oxford University Press, December 2015. Web. 16 January 2016.

Tao, F., Cheng, Y., Zhang, L., & Nee, A. Y. (2017). Advanced manufacturing systems: socialization characteristics and trends. Journal of Intelligent Manufacturing, 28(5), 1079-1094.

Thornhill, N. F., Patwardhan, S. C., & Shah, S. L. (2007). The CSTH simulation website, online: http://www.ps.ic.ac.uk/~nina/CSTHSimulation/index.htm. Accessed 29th July 2007.

Thornhill, N. F., Patwardhan, S. C., & Shah, S. L. (2008). "A continuous stirred tank heater simulation model with applications". Journal of Process Control, 18(3), 347-360.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003a). A review of process fault detection and diagnosis: Part I: Quantitative model-based methods. Computers & chemical engineering, 27(3), 293-311.

Venkatsubramanian, V., Rengaswamy, R., & Kavuri, S. N., (2003b). A review of process fault detection and diagnosis, Part II: Qualitative models and search strategics. Computers and Chemical Engineering, 27(3), 313-326.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S. N., & Yin, K. (2003c). A review of process fault detection and diagnosis: Part III: Process history based methods. Computers & chemical engineering, 27(3), 327-346.

VOLOŞENCU, C. (2015). "Fault Detection and Diagnosis in Industrial Systems, Based on Fuzzy Logic- A Short Review". Scientific and Technical Bulletin, Series: Electrotechnics, Electronics, Automatic Control and Computer Science, 2(1), 95-116.

Wang, J. X., & Roush, M. L. (2000). "What every engineer should know about risk engineering and management". CRC Press.

Yan, L., Xiwei, L., Noda, M., & Nishitani, H. (2007). Systematic design approach for plant alarm systems. Journal of Chemical Engineering of Japan, 40(9), 765-772.

Yang, F., Xiao, D., & Shah, S. L. (2009). Optimal sensor location design for reliable fault detection in presence of false alarms. Sensors, 9(11), 8579-8592.

Yang, F., Shah, S. L., & Xiao, D. (2010). SDG (Signed Directed Graph) based process description and fault propagation analysis for a tailings pumping process. IFAC Proceedings Volumes, 43(9), 50-55.

Yang, F., Shah, S. L., Xiao, D., & Chen, T. (2012). Improved correlation analysis and visualization of industrial alarm data. ISA transactions, 51(4), 499-506.

Zadakbar, O., Imtiaz, S., & Khan, F. (2012). Dynamic risk assessment and fault detection using principal component analysis. Industrial & Engineering Chemistry Research, 52(2), 809-816.

Zadakbar, O., Imtiaz, S., & Khan, F. (2013). "Dynamic risk assessment and fault detection using a multivariate technique". Process Safety Progress,32(4), 365-375.

Zhu, Q. X., & Geng, Z. Q. (2005). A new fuzzy clustering-ranking algorithm and its application in process alarm management. Chinese Journal of Chemical Engineering, 13(4), 477-483.